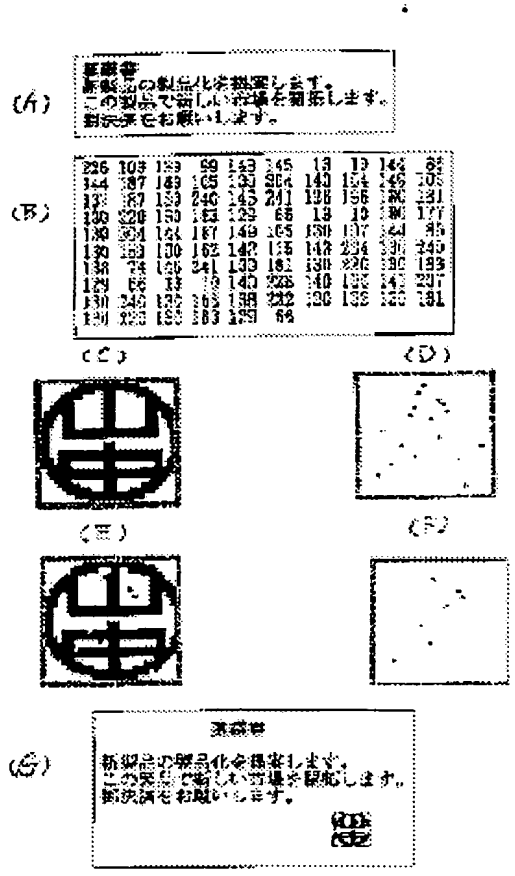
ELECTRONIC DOCUMENT SECURITY SYSTEM, ELECTRONIC STAMPING SECURITY SYSTEM AND ELECTRONIC SIGNATURE SECURITY SYSTEM

Patent number: JP10011509
Publication date: 1998-01-16
Inventor: FUKUZAKI YASUHIRO
Applicant: WACOM CO LTD
Classification:
- international: G06F17/60; G06F3/03; G06F15/00; G06T7/00; G06K17/00; G07F7/12; G09C1/00; H04L9/32
- european:
Application number: JP19960185484 19960626
Priority number(s):

Also published as:
US5948103 (A
JP10011509 (A

Abstract of **JP10011509**

PROBLEM TO BE SOLVED: To secure the strict authentication by adding a seal impression, a signature, etc., to a document and deforming the shapes of these seal impression, signature, etc., based on the feature value of the document. SOLUTION: A treatment device refers to the reference graphic data (C) on the seal prints, the signatures, etc., stored in a network server and applies a change (F) to the graphic data at a specific point (D) based on the feature value of the digest of the electronic document data. This result (E) can be recognized almost same as a reference graphic. At the verification side, the graphic data are separated from the approved electronic document data and the feature value that caused the change is calculated based on this graphic data and the reference graphic data. Then the coincidence is judged between the calculated feature value and the feature value that is obtained from the electronic document data.



(6)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10－11509

(43) 公開日 平成10年(1998)1月16日

(51) Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
G06F	17/60			G06F	15/21	Z	
	3/03	380			3/03	380 R	
	15/00	330			15/00	330 A	
G06T	7/00			G06K	17/00	L	
G06K	17/00		7259－5J	G09C	1/00	640 A	

審査請求 未請求 請求項の数 29 FD (全 26 頁) 最終頁に続く

(21) 出願番号 特願平8-185484

(22) 出願日 平成8年(1996)6月26日

(71) 出願人 000139403
株式会社ワコム
埼玉県北埼玉郡大利根町豊野台2丁目510番地1

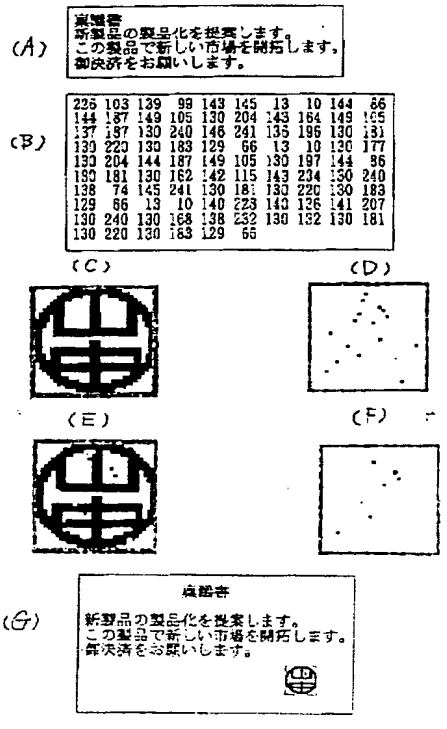
(72) 発明者 福崎 康弘
埼玉県北埼玉郡大利根町豊野台2丁目510番地1 株式会社ワコム内

(54)【発明の名称】電子書類セキュリティシステム、電子押印セキュリティシステムおよび電子署名セキュリティシステム

(57)【要約】 (修正有)

【課題】 印鑑やサインなどを文書に付加し、その形などを文書の特徴量で変形させることにより、厳密な認証を行う。

【解決手段】 処置装置側では、ネットワークサーバに保管されている印影やサインなどの基準図形データCを参照し、これに対し電子書類データのダイジェストなどの特徴量に基づき特定の点D上で変更Fを加える。結果Eは基準図形とほぼ同一と認識できる。検証側では、承認済み電子書類データから図形データを分離し、これと基準図形データとから変更の元になった特徴量を求め、電子書類データから得られる特徴量との一致を判定する。



1

【特許請求の範囲】

【請求項１】　電子的に作成された電子書類に対して承認者が電子的に承認を与える電子書類承認操作装置と、該承認された電子書類に対して検証者が該承認の正当性を電子的に検証する電子書類承認検証装置とからなる電子書類のセキュリティシステムであって、（イ）　前記電子書類承認操作装置が、

所定のソフトウェアで電子書類として再現可能な電子的な書類データを処理する電子書類データ処理手段と、

予め用意された基準となる図形データを参照する基準図形データ参照手段と、

前記電子書類データ処理手段に処理される電子的な書類データから該電子書類データに固有な特徴量を抽出する特徴抽出手段と、

該特徴抽出手段により抽出された特徴量に従って、前記基準図形データ参照手段により参照された基準図形データに変更を加えることにより変更図形データを生成する図形データ変更手段と、

該図形データ変更手段により生成された図形データを前記電子書類データ処理手段により処理される電子的な書類データに付加することにより承認済み電子書類データを生成する図形データ付加手段とからなり、（ロ）　前記電子書類承認検証装置が、

前記電子書類承認操作装置の図形データ付加手段により生成された承認済み電子書類データを処理する承認済み電子書類データ処理手段と、

前記電子書類承認操作装置の基準図形データ参照手段が参照した基準図形データと同一の図形データを参照する基準図形データ参照手段と、

前記承認済み電子書類データ処理手段により処理される承認済み電子書類データから、前記電子書類承認操作装置により付加された図形データと電子的な書類データとを分離するデータ分離手段と、

該データ分離手段により分離された電子書類データから該電子書類データに固有な特徴量を検出する特徴量検出手段と、

該図形データ分離手段により分離された図形データと、前記基準図形データ参照手段により参照された基準図形データとから、図形データの変更の元になった特徴量を求める図形データ変形特徴量再現手段と、

該図形データ変形特徴量再現手段から得られた特徴量と前記特徴量検出手段により検出された電子書類データ固有の特徴量との一致を判定する特徴量一致判定手段とからなることを特徴とする電子書類セキュリティシステム。

【請求項２】　前記図形データは、押印された印影を表わす図形であることを特徴とする請求項１の電子書類セキュリティシステム。

【請求項３】　前記図形データは、承認者の署名を表わす図形であることを特徴とする請求項１の電子書類セキュリティシステム。

2

【請求項４】　前記基準となる図形データは、２次元の点の色を示す情報であり、

前記図形データ変更手段は、その点の色を変更する手段であることを特徴とする請求項１から請求項３までのいずれかに記載の電子書類セキュリティシステム。

【請求項５】　前記基準となる図形データは、図形を構成する要素の位置や大きさを示す量を有しており、

前記図形変更手段は、図形を構成する要素の位置や大きさを変更する手段であることを特徴とする請求項１から請求項３までのいずれかに記載の電子書類セキュリティシステム。

【請求項６】　前記基準となる図形データは、持ち運び可能な媒体に保持されていることを特徴とする請求項１から請求項５までのいずれかに記載の電子書類セキュリティシステム。

【請求項７】　前記図形データ変更手段における変更は、撹乱データにより制御される撹乱処理を含むことを特徴とする請求項１から請求項６までのいずれかに記載の電子書類セキュリティシステム。

【請求項８】　前記撹乱データと、前記基準となる図形データとが、携帯可能な媒体に保持されていることを特徴とする請求項１から請求項７までのいずれかに記載の電子書類セキュリティシステム。

【請求項９】　前記図形データ変更手段と、前記基準図形データを有する媒体とが、ひとつの携帯可能な装置に内蔵されていることを特徴とする請求項１から請求項８までのいずれかに記載の電子書類セキュリティシステム。

【請求項１０】　電子押印装置と、電子押印検証装置とからなる電子押印セキュリティシステムであって、

（イ）　前記電子押印装置が、

所定のソフトウェアで電子書類として再現可能な電子的な書類データを処理する電子書類データ処理手段と、

予め用意された基準となる基準図形データを参照する基準図形データ参照手段と、

予め用意された公開鍵暗号化方式での暗号化用の秘密鍵データを保持する秘密鍵データ保持手段と、

前記電子的文書データを公開鍵暗号化方式での暗号化用の秘密鍵で暗号化する暗号化手段と、

前記暗号化手段で暗号化された文書データをパラメタとして、前記基準図形データを変形・修正する図形データ変更手段と、

前記文書データに前記図形データ変更手段で変形された図形データを付加する図形データ付加手段ととからなり、（ロ）前記電子押印検証装置が、

予め用意された基準となる基準図形データを参照する基準図形データ参照手段と、

前記図形データの付加された文書データから、文書データと、図形データとを分離する図形データ分離手段と、

該図形データ分離手段で分離された図形データと、前記基準図形データ参照手段により参照された基準図形データを比較して、暗号化された文書データを取り出す暗号化文書データ抽出手段と、

予め用意された公開鍵暗号化方式での復号化用の公開鍵データを参照する公開鍵データ参照手段と、

前記復号化用の公開鍵データを用いて、前記暗号化文書データ抽出手段で取り出された暗号化された文書データを復号化して平文の文書データにする復号化手段と、

前記図形データ分離手段から取り出された文書データと、前記復号化手段で復号化された文書データを比較して一致するかどうかを判定する一致判定手段とからなることを特徴とする電子押印セキュリティシステム。

【請求項１１】　電子署名装置と、電子署名検証装置とからなる電子署名セキュリティシステムであって、

（イ）　前記電子署名装置が、

所定のソフトウェアで電子書類として再現可能な電子的な書類データを処理する電子書類データ処理手段と、

予め用意された基準となる基準図形データを保持する基準図形データ保持手段と、

予め用意された公開鍵暗号化方式での暗号化用の秘密鍵データを保持する秘密鍵データ保持手段と、

前記電子的文書データを公開鍵暗号化方式での暗号化用の秘密鍵で暗号化する暗号化手段と、

前記暗号化装置で暗号化された文書データをパラメタとして、前記基準図形データを変形・修正する図形データ変更手段と、

前記文書データに前記図形データ変更手段で変形された図形データを付加する図形データ付加手段ととからなり、（ロ）前記電子署名検証装置が、

予め用意された基準となる基準図形データを参照する基準図形データ参照手段と、

前記図形データの付加された文書データから、文書データと、図形データとを分離する図形データ分離手段と、

該図形データ分離手段で分離された図形データと、前記基準図形データ参照手段により参照された基準図形データを比較して、暗号化された文書データを取り出す暗号化文書データ抽出手段と、

予め用意された公開鍵暗号化方式での復号化用の公開鍵データを参照する公開鍵データ参照手段と、

前記復号化用の公開鍵データを用いて、前記暗号化文書データ抽出手段で取り出された暗号化された文書データを復号化して平文の文書データにする復号化手段と、

前記図形データ分離手段から取り出された文書データと、前記復号化手段で復号化された文書データを比較して一致するかどうかを判定する一致判定手段とからなることを特徴とする電子署名セキュリティシステム。

【請求項１２】　前記暗号化用の秘密鍵データを携帯可能な媒体に格納したことを特徴とする請求項１０又は請求項１１のいずれかに記載のセキュリティシステム。

【請求項１３】　前記暗号化用の秘密鍵と押印又は署名時に使用される基準図形データを携帯可能な媒体に格納したことを特徴とする請求項１０又は請求項１１のいずれかに記載のセキュリティシステム。

【請求項１４】　前記暗号化手段と秘密鍵データ保持手段を電子押印又は電子署名装置から分離して、別の携帯可能な装置としたことを特徴とする請求項１０又は請求項１１のいずれかに記載のセキュリティシステム。

【請求項１５】　前記基準図形データの保持手段も携帯可能な装置に搭載したことを特徴とする請求項１４のセキュリティシステム。

【請求項１６】　前記押印又は署名検証装置で使用する基準図形データが、電子押印又は電子署名装置で使用する基準図形データとは内容は同じでも、別々に保持されていることを特徴とする請求項１５のセキュリティシステム。

【請求項１７】　前記携帯可能な媒体または装置は、物理的な印鑑（実際の印章）の外観形状をしていることを特徴とする請求項１２から請求項１６までのうちのいずれかに記載のセキュリティシステム。

【請求項１８】　押印または署名の位置を位置を指示する位置指示器と、その指示位置を検出する座標検出手段とを有することを特徴とする請求項１１から請求項１７までのいずれかに記載のセキュリティシステム。

【請求項１９】　前記携帯可能な媒体が、前記位置指示器に内蔵されていることを特徴とする請求項１８のセキュリティシステム。

【請求項２０】　前記位置指示器と前記座標検出手段とはそれぞれ相互に通信手段を有し、前記内蔵された媒体に格納された秘密鍵データ、または基準図形データを、前記通信手段によって、電子押印又は電子署名装置に伝達することを特徴とする請求項１９のセキュリティシステム。

【請求項２１】　電子押印装置と、押印検証装置とからなる電子押印セキュリティシステムであって、（イ）前記電子押印装置が、

所定のソフトウェアで再現可能な電子的文書データを処理する電子文書処理手段と、

予め用意された基準となる基準図形データを保持する基準図形データ保持手段と、

予め用意された公開鍵暗号化方式での暗号化用の秘密鍵データを保持する秘密鍵データ保持手段と、

前記電子文書処理手段により処理される電子的文書データから、その文書の特徴を取り出して文書特徴データを作成する文書特徴データ抽出手段と、

該文書特徴データ抽出手段により抽出された文書特徴データを前記秘密鍵データ保持手段により保持された秘密鍵で暗号化する暗号化手段と、

該暗号化手段により暗号化された文書特徴データをパラメタとして、前記基準図形データを変更する図形データ

変更手段と、
前記電子文書処理手段により扱われる電子的文書データに前記図形データ変更手段により変形された図形データを付加することにより押印済み電子文書を生成する図形データ付加手段とから構成され、（ロ）　前記押印検証装置が、
前記図形データ付加手段により生成された押印済み電子文書から、文書データと図形データとを分離する図形データ分離手段と、
前記基準図形データ保持手段により保持される基準図形データと同一の基準図形データを参照する基準図形データ参照手段と、
該基準図形データ参照手段により参照された基準図形データと、前記図形データ分離手段により分離された図形データとを比較して、暗号化された文書特徴データを取り出す暗号化文書特徴データ抽出手段と、
予め用意された公開鍵暗号化方式での複号化用の公開鍵データを保持する公開鍵データ保持手段と、
該公開鍵データ保持手段により保持された公開鍵データを用いて、前記暗号化文書特徴データ抽出手段により取り出された暗号化された文書特徴データを復号化して元の文書特徴データを取得する復号化手段と、
前記図形データ分離装置により分離された文書データから、前記電子押印装置の文書特徴データ抽出手段と同一の方法により、文書の特徴を取り出して文書特徴データを作成する文書特徴データ抽出手段と、
該文書特徴データ抽出手段から得られた文書特徴データと、前記復号化手段から取得された文書特徴データとを比較して一致するか否かを判定する文書特徴データ一致判定手段とから構成されることを特徴とする電子押印セキュリティシステム。
【請求項２２】　電子署名装置と、署名検証装置とからなる電子署名セキュリティシステムであって、（イ）　前記電子署名装置が、
所定のソフトウェアで再現可能な電子的文書データを処理する電子文書処理手段と、
予め用意された基準となる基準図形データを保持する基準図形データ保持手段と、
予め用意された公開鍵暗号化方式での暗号化用の秘密鍵データを保持する秘密鍵データ保持手段と、
前記電子文書処理手段により処理される電子的文書データから、その文書の特徴を取り出して文書特徴データを作成する文書特徴データ抽出手段と、
該文書特徴データ抽出手段により抽出された文書特徴データを前記秘密鍵データ保持手段により保持された秘密鍵で暗号化する暗号化手段と、
該暗号化手段により暗号化された文書特徴データをパラメタとして、前記基準図形データを変更する図形データ変更手段と、
前記電子文書処理手段により扱われる電子的文書データ

に前記図形データ変更手段により変形された図形データを付加することにより署名済み電子文書を生成する図形データ付加手段とから構成され、（ロ）　前記署名検証装置が、
前記図形データ付加手段により生成された署名済み電子文書から、文書データと図形データとを分離する図形データ分離手段と、
前記基準図形データ保持手段により保持される基準図形データと同一の基準図形データを参照する基準図形データ参照手段と、
該基準図形データ参照手段により参照された基準図形データと、前記図形データ分離手段により分離された図形データとを比較して、暗号化された文書特徴データを取り出す暗号化文書特徴データ抽出手段と、
予め用意された公開鍵暗号化方式での複号化用の公開鍵データを保持する公開鍵データ保持手段と、
該公開鍵データ保持手段により保持された公開鍵データを用いて、前記暗号化文書特徴データ抽出手段により取り出された暗号化された文書特徴データを復号化して元の文書特徴データを取得する復号化手段と、
前記図形データ分離装置により分離された文書データから、前記電子署名装置の文書特徴データ抽出手段と同一の方法により、文書の特徴を取り出して文書特徴データを作成する文書特徴データ抽出手段と、
該文書特徴データ抽出手段から得られた文書特徴データと、前記復号化手段から取得された文書特徴データとを比較して一致するか否かを判定する文書特徴データ一致判定手段とから構成されることを特徴とする電子署名セキュリティシステム。
【請求項２３】　前記秘密鍵データ保持手段を携帯可能な媒体に格納したことを特徴とする請求項２１または請求項２２のいずれか記載のセキュリティシステム。
【請求項２４】　前記秘密鍵データ保持手段と、前記基準図形データ保持手段とを携帯可能な媒体に格納したことを特徴とする請求項２１または請求項２２のいずれかに記載のセキュリティシステム。
【請求項２５】　前記暗号化手段と秘密鍵データ保持手段とを、前記図形データ付加手段から分離して、別の携帯可能な装置としたことを特徴とする請求項２１または請求項２２のいずれかに記載のセキュリティシステム。
【請求項２６】　該携帯可能な装置に、前記基準図形データの保持手段をも搭載したことを特徴とする請求項２５に記載のセキュリティシステム。
【請求項２７】　押印または署名の位置を指示する位置指示器と、
その指示位置を検出する座標検出手段とを有することを特徴とする請求項２１から請求項２６までのいずれかに記載のセキュリティシステム。
【請求項２８】　前記携帯可能な媒体が、前記位置指示器に内蔵されていることを特徴とする請求項２７に記載

のセキュリティシステム。

【請求項２９】　前記位置指示器と前記座標検出手段とはそれぞれ相互に通信手段を有し、前記内蔵された媒体に格納された秘密鍵データ、または基準図形データを、該通信手段によって、電子押印／電子署名装置に伝達することを特徴とする請求項28に記載のセキュリティシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子的な書類におけるセキュリティ技術に関するものである。

【０００２】

【従来の技術】最近、ＬＡＮの普及により、会社内での電子的な書類のやりとりが多くなってきている。しかしながら、そのような書類の決済や承認といった処理は、電子的に行うことが難しいのが現状である。物理的な書類であれば、印鑑を押して決済するのが日本の慣行であるし、欧米ではサインがこれに代るものである。このような印鑑やサインをコンピュータ上で再現することは大変簡単なことであるが、電子的な情報であるので、複製や改竄が極めて容易となり、セキュリティ上の問題が発生する。そこで、現在、使われているのが、いわゆる暗号化技術である。特に最近開発された暗号化方式として公開鍵暗号化方式がある（特公平６－２０１９９、特開平２－１３４９４０、特開平３－６７３５６、特開平３－１９５２２９、特開平４－９１５３１、特開平４－１１８７７７、特開平４－１６０４９３、特開平５－２６００４３、特開平６－９５５９１、特開平６－１０３４２５、特開平６－１０３４２６、特開平６－１５００８２、特開平６－１６１３５４、特開平６－１６２２８９、特開平６－２２４８９６、特開平６－３１５０３６、特開平７－１３５６８０、特開平７－１６２４５１）。従来の共通鍵暗号化方式では、二つの鍵を使い、その一方を公開することによって、情報送信者の特定と情報受信者の特定が別々に可能になった。つまり、秘密鍵で暗号化した文書を公開することで、文書の内容は公開しながらも、その文書は他の人間が作成したものではなく、改竄もされていないことを保証するという、まさに従来のサインに近い用い方ができるようになった。これが、デジタル署名あるいは電子シグネチャと呼ばれるものである。また、暗号化してしまうと、その内容が平文で読めなくなってしまうので、単に改竄の防止だけが目的で、内容自体を秘密にする必要のない場合は、その文書を暗号化した文字が、元の文書に付け加えられる形で、使用されている。これをクリア・シグネチャと呼ぶことにする。

【０００３】さて、実際には、公開鍵暗号化方式は処理が複雑で、高度な処理能力を必要とし、従来の暗号化処理より時間がかかるタイムコンシューミングプロセスであるとされている。そこで、文書を直接暗号化するのではなく、文書から特徴データを取り出して、その取り出された短いデータを暗号化する方法が用いられている。この取り出された特徴データは、電子の指紋とも呼ばれ、元の情報が１ビットでも異なれば、推測不能な全く別のデータが取り出される。これには、一方向性ハッシュ関数が用いられており、実際に、ＭＤ２、ＭＤ４、ＭＤ５といったプログラムが米国ＲＳＡ　ＤＡＴＡ　ＳＥＣＵＲＩＴＹ，Ｉｎｃ．から、公開されている。ＲＳＡデータセキュリティ社の特徴抽出プログラムに関する公開文書は、「Ronald Rivest,"The MD5 Message-Digest Algorithm",RFC-1321 MIT Laboratory for Computer Science, 1991.」がある。この文書は、ＲＳＡデータセキュリティ社自身によりインターネット上で公開されている。この中に実際に動作するソースコードが含まれており、実際に本願の発明者のコンピュータ環境によっても動作が確認された。このＲＳＡデータセキュリティ社のプログラムは、可変長の原文データを１２８ビット固定長の特徴データに変換するものである。ＭＤ２やＭＤ５は、実際の公開鍵暗号化通信ソフトであるＰＧＰや、暗号化電子メールの規格であるＰＥＭなどで、採用されているものである。

【０００４】図１１は、従来から存在する電子シグネチャ（クリアシグネチャ）を示す図である。図１１（Ａ）は、署名の対象となる文書を示す。図１１（Ｂ）は、署名の対象となる文書を示す平文の後に続けて電子署名（デジタル署名、電子シグネチャ）を施したものである。この電子署名は、発信者の秘密鍵により文書を暗号化したものである。受信者は、公開鍵により復号化して平文と同様の文書が得られることを確認することにより、当該電子書類の真正であることを検証できる。

【０００５】公開鍵暗号化方式以外の特徴データの求め方としては、古いものではいわゆるチェックサムと呼ばれる方法がある。これは、データが文字コード等を表すものであるか否かに拘らず、それらをすべて数値とみなして加算し、その合計をもって、特徴データとするものである。これは、非常に簡単に特徴データを求めるやり方ではあるが、セキュリティ機能は脆弱である。

【０００６】

【発明が解決しようとする課題】クリア・シグネチャとして付加される文は、意味不明の文字の羅列となり、見方によってはたいへん目障りである。

【０００７】また、クリア・シグネチャを作成するときに使われる秘密鍵データは通常、その装置に組み込まれており、その秘密鍵の管理が重要な問題となる。

【０００８】ところで、物理的な書類に対しては、図１１（Ｃ）に示すように、印鑑やサインが使われてきたのであり、もし、電子的な書類に付加されるものが、そのような形態をしていれば、たいへん自然であり、しかも、人間がその内容を一応は判断ができるようになる。

【０００９】

【課題を解決するための手段】そこで、印鑑やサインなどの情報を付加することで、人間の目にもその書類が真正のものであるらしいことについてのある程度の判断ができ、また、その印鑑やサインの形などを文書の特徴量で変形させることにより、厳密な認証を行うことができるようにしようというのが、本発明の内容である。

【００１０】もし、図形を２次元の点の集合、いわゆるビットマップ、で表わすとすれば、その点の一部またはすべてを、文章の特徴量で変化させることにより、特徴量の情報を反映させることができる。

【００１１】また、図形が、線や円、矩形といった要素図形の位置や大きさ、つまり、いわゆるベクトル情報で構成されている場合は、その要素図形の位置や大きさに文章の特徴量を反映させることができる。

【００１２】このようにしておいて、本当に複製や改竄が行われていないかを検証する必要のある場合は、文章の特徴量によって変形された図形データから、逆に文章が持っているはずの特徴量を引き出して、文書自体の特徴量と比較すればよい。

【００１３】ここでいう文章は、文字を表わす情報のみで構成されていることに限定されない。図形情報や、音声情報、動画などのマルチメディア情報、あるいは他の文書への参照情報を含むいわゆるハイパーテキストであっても、かまわない。

【００１４】また、例えば、下級の管理者によって、印や、サインが、本願でいうセキュリティ機能を伴って使われている文書の印やサインを含む全体を新たな文書と見なして、上級の管理者がさらに本発明の印やサインをすることで、さらにセキュリティが強化される。

【００１５】ここでいう特徴量とは、上述の電子指紋データやチェックサムのような方式で取り出されるデータのことである。この特徴量を公開鍵暗号化方式の秘密鍵で暗号化して、暗号化後のデータで図形を変形させるようにすれば、強力なセキュリティが実現できる。

【００１６】あるいは、暗号化まではしなくても、単に特徴量で変形させるだけであっても、単純な図形コピーを防止することができる。つまり、コンピュータ上では、素人でも、図形データをいとも簡単にコピーすることができるという問題があるが、そのような行為に対しては、これだけでも効果的である。

【００１７】さらに、特徴量データを図形データの変形に反映させる際の反映させる点や反映の仕方などを変化させることで、偽造は困難になる。ここでは、この操作を撹乱処理と呼び、撹乱用のデータを撹乱データと呼ぶ。つまり、元のデータは視認性を保持するためにある程度固定しておく必要があるので、これを固定して公開しておき、別に秘密の撹乱データを有し、それに基づいて撹乱することで、セキュリティを高めようとする方法である。ここでいう撹乱は、暗号化の一種と見ることもできる。その場合の撹乱データは暗号鍵データのことに

なる。但し、実際に図形データの中のどの点がどのように変化するのかを指定し、かつ視認性が失われないように制限を加えることを示す情報が何らかの形で必要になる。もし、公開鍵暗号化のような本格的な暗号化手段でセキュリティ強度そのものが確保されているのであれば、視認性を保つために変化点位置を制限したりする情報は、元になる図形データそのものに埋め込んでおくことも可能である。つまり、ビットマップで変化する位置の点の色を予め変えておくことなどがその例である。

【００１８】もし、印影を使うのであれば、それを押印する道具は実際の印鑑の形をしていたほうが分かり易い。実際、タブレットと呼ばれる位置検出装置において、印鑑の形状をした位置指示器（電子印鑑）を使用すれば、実際の印鑑にかなり近い操作感覚が得られる。その電子印鑑の中に、印影データやここでいう撹乱データなどを搭載すれば、セキュリティ機能を持った電子印鑑システムとなる。

【００１９】また、サインを使う場合、サインする道具はペンである。ペンについてもそれを電子化したもの（電子ペン）が、タブレット上で使用可能である。ただし、その場合に実際にサインをその都度手書きで入力していたのでは、この特許の主旨には合わない。その都度違う図形では基準図形データとして扱うことができないからである。本発明における基準図形データは一般のサインのように単にいつどこでかいても同様の特徴を持った筆跡で書けるというだけでは足りず厳密にその図形を表す電子データが電子的に見て同一であって完全一致するものでなければならない。従って、あるときある場所でタブレット等により取得されたサイン筆跡のデータをその後も用いることになる。つまり、サインをその都度記入するのではなくサインデータを電子ペンに貯えておいて、そのデータをコンピュータに渡すといった用い方になる。

【００２０】また、このような電子印鑑や電子サインにおいて、そのオリジナルの印影データやサインデータまたは撹乱データから、実際に電子書類に追加される図形データを作成する処理を、その場にあるコンピュータで行う場合、オリジナルの印影データやサインデータ、撹乱データを一旦、コンピュータで受け取ることになる。それで、例えば、外出先のコンピュータで使う場合などに、本来は秘密にしなければならないデータを本人の意に反してコピーされて悪用される可能性は否定できない。

【００２１】そこで、そのような場合も含めて、もっとも安全なのは、電子印鑑、もしくは電子ペンの中で、図形データの変形処理を行う事である。電子印鑑もしくは、電子ペンは、文書データ自体か、文書データの特徴量データを受け取って、その特徴量を反映ずみの図形データをコンピュータに送り返せばよい。このような事を実現するためのハードウェア構成については、後述する

ように、本出願人が別途、特許出願している。

【００２２】

【発明の実施の形態】以下、発明者が最良と思う実施の形態を述べる。

【００２３】セキュリティ強度を現在考えられる限り最大にするために公開鍵暗号化方式を用いる。この公開鍵暗号化方式での秘密鍵で平文の文書データを暗号化する。その際具体的には、ハッシュ関数などで、特徴を保ったままデータを一旦縮小しておいて、その縮小したデータを暗号化する方が効率がよい。元の文書データを平文データ、暗号化した後のデータを暗号化データと呼ぶ。この暗号化データで基準図形データを変形または修正して、元の平文データに付加する。ここまでが、電子押印または電子署名の手段となる。

【００２４】次がその押印または署名された平文データを受け取った人が、その押印または署名の正当性を検証する手段である。まず、付加された図形データと元の基準図形データを比較して、暗号化データを抽出する。そして、抽出された暗号化データを公開鍵で復号化して、元の平文データを得る。こうして得られた平文データと受け取った平文データを比較することで、その押印または署名の正当性が確認できる。特徴量データをもって比較を行う場合には、平文データから抽出した特徴量データを、図形データから抽出した特徴量データと比較することになる。

【００２５】基準図形データ及び公開鍵は、押印または署名されたデータを検証する人が自由に入手できるようになっている必要がある。

【００２６】ここで、秘密鍵データを移動可能な媒体に保持しておけば、秘密鍵の管理が簡単になる。また暗号化装置と秘密鍵データを同一の携帯可能装置に搭載しておけば、秘密鍵データがその装置の外に出ないので、セキュリティレベルは最高となる。

【００２７】位置指示器内部に暗号化装置と秘密鍵データを搭載して、押印／署名の位置を位置検出装置で指示しながら、データ通信を行い押印／署名操作をなすようにすることができる。

【００２８】暗号化されたデータ量は短い文（５０文字程度）でも、１Ｋビット以上になる。一方、印鑑の印影の大きさは縦横６４ビットづつで、４Ｋビットあるので、そのドットの４つにひとつの割合で反映させればよい。もし、それで、印影がくずれて、人間にとって判別しずらくなるようであれば、各点の色のデータを使えばよい。例えば、今のWindows（米国マイクロソフト社の商標）のような環境では２５６種類の色が設定可能であるので、これを８ビットの情報とみれば、先程の６４ドット四角の印影データは３２Ｋビットのデータを持つ事になり、１Ｋビット程度の情報を反映させても、印影の判別は可能である。また、元の文書が長い場合には、そのすべてをそのまま暗号化するのではなく、要点を短くまとめた文を付け加えて、それを暗号化すればよい。

【００２９】また、サインの場合、そのサインを構成するベクトルデータの点の数が５００点として、それぞれの点がＸ方向とＹ方向に±３ドットずつ動かせるとすると、７×７で４９点で約５．５ビットの情報量となるので、５００点で２７５０ビット表現できるので、１Ｋビット程度の変形情報を反映させる事ができる。ここでは、前述のＭＤ２やＭＤ４、ＭＤ５などの特徴量抽出手段を使わない場合の、データ量の概算を示した。なお、前述の特徴量抽出手段を用いれば、どんな大きなデータもわずか１２８ビットの特徴データとすることができるので、その場合のデータ量の制限は特になく、ＣＰＵの処理速度の問題のみとなる。

【００３０】さらに、入力面と表示面が一体になったシステム、つまり、位置検出装置と表示装置とが積層配置されて一体になっているものを用いて、その上で印鑑型の位置指示器を画面に押し付ければ、その場に印影が表示され、その印影のかすれ具合が、実は文書の暗号化データを含んでおり、電子的に検証ができるというシステムが、構築可能である。

【００３１】

【実施例】以下、本発明の実施例について図面を参照しつつ説明する。図１は本発明に係る電子書類セキュリティシステム、電子押印セキュリティシステムまたは電子署名セキュリティシステムの基本構成を示す機能ブロック図である。機能ブロック図を用いたのは、本発明が多くの場合、汎用コンピュータ間のデータのやり取りに関して適用されるものであり、ブロック図に示される「特徴量抽出部」、「図形データ変更手段」、「特徴量再現部」、「特徴量一致判定部」等の各構成部分は情報処理機器としてのコンピュータ（厳密にいえばコンピュータのセントラルプロセッシングユニットすなわちＣＰＵ）がその機器内に設けられた記憶装置にあらかじめ記憶されたプログラムを読み込んでその手順を実行することによりその都度実現するものであること、すなわちソフトウェアにより実現されるものである場合が多いことに基づく。ワードプロセッサ専用機器や、多機能電話機、他の通信機器等の専用機により実現する例を排除するものではない。このことは図６から図１０までの他の機能ブロック図についても同様である。

【００３２】図１に描かれた破線で囲んだ二つの装置、電子押印または電子サイン処理装置１００と電子押印または電子サインの検証処理装置２００とは本発明に係る電子書類セキュリティシステム、電子押印セキュリティシステム又は電子署名セキュリティシステムを構成する二つの装置である。「電子押印処理装置」又は「電子サイン処理装置」というネーミングは従来紙の書類に対して印鑑又はサインにより行っていた書類承認操作を電子的に処理する装置であるという観点からのネーミングである。「電子押印処理装置」と「電子サイン処理装置」と

の双方を含む上位の概念を抽出すれば、「電子書類承認操作装置」と捉えることのできるものである。同様に「電子押印検証処理装置」又は「電子サイン検証処理装置」というネーミングは従来印鑑の押印又はサインの実行された紙の書類に対して目視にてそれが確からしいこと(本人がまさに押印又はサインをしたものであること)を検証してその書類の真正であることを確かめていた操作を電子的に処理する装置であるという観点からのネーミングである。「電子押印検証処理装置」と「電子サイン検証処理装置」との双方を含む上位の概念を抽出すれば、「電子書類承認検証装置」と捉えることのできるものである。

【００３３】また、図１に描かれた二つの装置は通常は一つの筐体を有する装置(一つのコンピュータ）の中に「承認」と「検証」との双方の機能を併せ持つような装置が複数存在し、それらの装置のうちの二つの間で「承認」と「検証」の操作がなされる場合において、一方の装置中の「承認」の機能にのみ着目し、他方の装置中の「検証」の機能にのみ着目して描いたものと見ることができる。ちょうど二つのトランシーバーの間で通話をするときに双方とも送信、受信の両機能を持っているが一方が送信しており、他方が受信している状況に着目して一方の送信機能と他方の受信機能とのみを問題としているがごとくである。したがって、電子押印又は電子サイン処理装置１００における特徴量抽出部１１０と電子押印又は電子サインの検証処理装置２００における特徴量抽出部２１０とは同一の機能を有するものであるが、違う個体としての情報処理装置に設けられたものである。言い換えれば、図１の電子押印又は電子サイン処理装置１００に設けられた特徴量抽出部１１０は、それが属するコンピュータが「承認」操作をする立場のときには、特徴量抽出部１１０の役を演じるが、一旦それが属するコンピュータが「検証」処理をする立場に立てば、特徴量抽出部２１０の役割を演じる可能性を秘めたものであるといえる。

【００３４】図１に示された電子押印又は電子サイン処理装置１００と電子押印又は電子サイン検証処理装置２００とから構成される電子書類セキュリティシステム、電子押印セキュリティシステム又は電子署名セキュリティシステムに関し、主にデータの処理の流れにしたがって、このセキュリティシステムの構成及びその働きを説明する。文書データＤ００１は、所定のソフトウェアで電子書類として再現可能な電子的な書類データである。ここで、所定のソフトウェアとは例えばワードプロセッサ、表計算、データベース、ＣＡＤ(コンピュータエイディッドデザイン)、あるいは社内メールシステム等のコンピュータのアプリケーションプログラムであって、電子的な書類データを確実に保存でき、かつ、ＣＲＴ(陰極線管：カソードレイチューブ）装置等に表示してあたかも紙の書類を見るかのように操作者の肉眼によるビジュアルな形に現わすことのできるソフトウェアを指す。

【００３５】文書データＤ００１が電子押印又は電子サイン処理装置１００に引き渡される経路はいくつか考えられる。第一に、文書データＤ００１を作成した者が自らその電子書類に電子的な押印、電子的なサイン等の承認操作を施そうとする場合には、文書データＤ００１は、電子押印又は電子サイン処理装置１００を構成するコンピュータの記憶装置にすでに記憶されていると考えられる。したがってその場合には当該ファイルにアクセスすることをもって文書データＤ００１は電子押印又は電子サイン処理装置１００に引き渡される。第二に、文書データＤ００１を作成した者が承認者とは異なる場合であって、その二人の用いるコンピュータが特には接続されていないような場合には、フロッピーディスク等の情報記憶媒体を通して承認者の用いるコンピュータに持ち込まれ、当該コンピュータに組み込まれた電子押印又は電子サイン処理装置１００がアクセス可能な状態となる。第三に、文書データＤ００１の発信者と承認者のそれぞれ用いるコンピュータがローカルエリアネットワーク又はモデムと電話回線を通じたネットワーク等により接続状態にある場合には電子メールシステム等により発信者が承認者に対して文書データＤ００１を送り、承認者はそれを受信するという形式により文書データＤ００１の引き渡しがなされ得る。電子押印又は電子サイン処理装置１００に引き渡された文書データＤ００１は、少なくとも一時的に(必要があれば半永久的に)電子押印又は電子サイン処理装置１００に記憶されるべきであるから電子押印又は電子サイン処理装置１００は電子書類データ記憶手段を有する。煩雑を避けるため図１には描くのを省略した。

【００３６】図１に示す文書データＤ００１は、操作者が見えるように表示装置にビジュアルに表示した場合には、図２（Ａ）に示すような日本語の文書又は図３（Ａ）に示すような英語の文書（他の言語による文書でも構わない）であるが、電子的なデータとしてみれば、図２（Ｂ）又は図３（Ｂ）に示すような文字コードを表す数字の羅列となる（図２及び図３については後述する）。特徴量抽出部１１０は、文書データＤ００１の文書データとしての特徴、すなわち文字コードの数字の羅列としての特徴量を抽出する。この特徴量抽出は後で図２及び図３を参照しつつ詳述するように例えばチェックサムを用いてすることができる。特徴量抽出部１１０により抽出された文書データＤ００１の特徴量はそれに基づいて図形データを変更すべく、図形データ変更手段１２０に送られる。図形データ変更手段１２０は、図形データＤ００２を読み込んでそれに対して文書データＤ００１の特徴量に応じた変更を加える。変更を加えられた図形データは文書データＤ００１に追加されて「文書データ」に「文書データの特徴量により変形された図形データ」が付加されたデータＤ００３として出力される。

このように、文書データＤ００１と図形データＤ００２とからＤ００３を生成する装置が電子押印又は電子サイン処理装置１００であるということができる。電子押印又は電子サイン処理装置１００には、文書データＤ００１に変形された図形データを付加する図形データ付加手段が内在するとみるべきであるが、図１では、煩雑を避けるため図示を省略した。また、図１に示した図形データＤ００２には、括弧書きで撹乱データを記載しているが、この意味については後述する。

【００３７】電子押印又は電子サインの検証処理装置（前述したように「電子書類承認検証装置」と見ることもできる）２００は、図１の下半分に描かれた破線に囲まれた部分であり、主に特徴量抽出部２１０、特徴量再現部２２０、特徴量一致判定部２３０とからなる。電子押印又は電子サインの検証処理装置２００は、「文書データ」に「文書データの特徴量により変形された図形データ」の付加されたデータＤ００３と図形データＤ００２との二つのデータを取得して、Ｄ００３のデータの正当性、即ちＤ００１に加えられた承認の正当性を検証する装置である。従って、その手順はまず、Ｄ００３とＤ００２との二つのデータを取得するところから始まる。この意味において、電子押印又は電子サインの検証処理装置２００は承認済み電子書類データ記憶手段と基準図形データ参照手段（図形データＤ００２は変更が加えられていない図形データなので基準図形データと見ることができる。以下、変更された図形データとの区別を意識するときは、必要に応じてＤ００２を基準図形データともよぶことにする。）とを内在するといえる。基準図形データの参照の仕方は、後述するように、例えばネットワークサーバを介して当該データを参照するといったやり方が考えられる。これら二つの手段は、図１に図示することは省略して煩雑を避けた。

【００３８】電子押印又は電子サインの検証処理装置２００に取り込まれたＤ００３は、文書データと「文書データの特徴量により変形された図形データ」とに分離されて、文書データは特徴量抽出部２１０に送られ、「文書データの特徴量により変形された図形データ」は特徴量再現部２２０に送られる。この意味において電子押印又は電子サインの検証処理装置２００はデータ分離手段をも内在するとみるべきであるが、この分離は単にくっついているのを分けるだけであり、通常は簡単な処理である。近時のワードプロセッサやメイルシステム等のアプリケーションプログラムは文書データと図形データとの混在するデータを扱うのを得意としており、その混在データを表示装置にビジュアルに表示する際にも両者の混在するものであることを操作者に意識させることなく表示するのが通常である。Ｄ００３のデータが二つのデータの付加されたデータであることは、このような意味における付加であるから、その分離もまたここでは簡単な処理である。したがって、このデータ分離手段は本発

明の大筋からは遠いため煩雑を避ける意味で図１からは図示を省略した。

【００３９】さて、電子押印又は電子サインの検証処理装置２００が、Ｄ００３の正当性を検証するやり方は、文書データの特徴量を二つの方法で抽出して、それらが一致するか否かを判定することにより行われる。まず、特徴量抽出部２１０は、Ｄ００３から分離された文書データ、即ち元々の文書データＤ００１と同一の文書データから特徴量を抽出する。こうして得られた特徴量は、電子押印又は電子サイン処理装置１００が文書データＤ００１から得た特徴量と同一のはずである。一方、特徴量再現部２２０は、「文書データの特徴量により変形された図形データ」と「基準図形データ（Ｄ００２）」とから特徴量を再現する。この再現が可能であるためには、電子押印又は電子サイン処理装置１００において図形データ変更手段１２０が加えた変更が特徴量に対して一意的であるか、あるいは、その図形データ変更からもとの特徴量への変換の解が常に求めることのできるものであって、その解の個数が有限であれば足りる。一意的である場合には、まさにそれらの二つの特徴量が完全一致するか否かを特徴量一致判定部２３０は比較し、判定すればよい。一意的でない場合は、有限個のその解のうちのいずれかに一致することをもって特徴量が一致したとして押印又はサインの正当性を検証することとなる。口述する図６から図１０までにおける特徴量一致判定もこの意味における一致で足りる。一意的である場合の方が、一意的でない場合に比べて処理が簡単であり、かつ検証の確からしさの度合いも大きいので望ましいといえる。

【００４０】図２及び図３を参照しつつ、文書データや図形データの実例に即して説明する。図２は、文書データが日本語文書データ、図形データがビットマップデータである場合について本発明に係る書類承認、承認検証のやり方を示した図である。図２（Ａ）は、日本語文書の一例を示したものである。図２（Ｂ）は、図２（Ａ）の日本語文書を構成する各文字をシフトＪＩＳコードによりコード化したデータである。漢字は２バイトコードとなり、この文書全体で９６バイトとなる。この文字データを表す数字は厳密にいえば序数であって、数値ではないともいえるが、これらをすべて数値とみなして加算したものが、いわゆるチェックサムと呼ばれるものとなる。この例でいえば文字データの加算合計は、１３８６４（１０進数）となる。これを２進数に表すと、００１０１１０００１０１０００（２進数）となる。例えば、この量を文書データの特徴量とすることができる。

【００４１】図２（Ｃ）は、ビットマップで構成されている図形データを示している。これは、基準図形データ（図１で示したＤ００２）である。ここでは、日本国などで紙の書類の承認に用いられている印鑑の押印図形（印影）を示す図形をビットマップで電子的データとし

て表現したものを用いている。署名の筆跡（シグネチャ）をビットマップで表現して基準図形データとすることもできるし、トレードマーク、ロゴマーク、紋章、記章等のマークを用いることもできる。日本国で用いられる印鑑に類似したものに限らず欧米で用いられることのある封印に類似したものを用いることもできる。印影を示す図形はここでは効果を見やすくするために縦３２ドット、横３２ドットとしている。図２（Ｃ）に示すようにここでは「山中」という日本人の名前の姓を表す印影があり、図２（Ｄ）に示すようにここでは１６個の点を文字データの特徴量データを反映させる点（ビット）として予め定めておく。この１６個の点がどの点（ビット）であるかを示す情報は図１に示すＤ００２（基準図形データ）に含まれる。図形データの中で、実際に特徴量データを反映させる位置を示すデータは、後述するように撹乱データとして用いられるものであり図１に示したＤ００２では括弧書きで示したものである。さきほどのチェックサムの結果得られた１６ビットの２進数に基づいて基準図形データのうちの１６点のそれぞれに変更を加える。例えば、各ビットが１ならば白黒反転、０ならば変更無しと割り当てることができる。そのようにして上記「００１１０１１０００１０１０００」に基づいて図２（Ｃ）の基準図形データのうちの図２（Ｄ）に示す１６点に変更を加えた結果が図２（Ｅ）であり、その１６点のうち白黒反転させた点のみを抜き出して表示したのが図２（Ｆ）である。このようにして得られた図２（Ｅ）の図形は、文書データの特徴量を含み、かつ人の目には、印影とほぼ同一のものとして判別できるものとなる。この変形された図形データを文書データに追加したものが、図２（Ｇ）となる。図２（Ｇ）は日本国等において従来の紙の書類文化の慣行上通常なされてきた書類に押印するという処理を電子的に行った結果を実現したものといえる。

【００４２】さて、逆にこの印影から、元の文書の特徴量を求めるには、元の基準図形データ（印影データ）と照合して、特徴量を反映させるべき点（ここでは１６点）の状態から、特徴量を再現することができる。元の基準図形データは、印鑑に代わるものであるからその所持すべき者が厳重に保管すべきであるが、他人に対しては検証処理において特徴量を抽出する処理のためにだけ参照される。このような基準図形データの管理は、例えば、ネットワークサーバにおいて基準図形データを管理することによってなされ得る。図１に示す特徴量再現部２２０によって再現された特徴量と、図１に示す特徴量抽出部２１０が文書データから再度抽出した特徴量との一致を確認すれば、その文書が改竄されていないことが分かる。また、同時に印影が他の文書からコピーされたものではないことも判明する。

【００４３】ここでは、説明のため、特徴量を求める手段として、もっとも簡単な方法であるチェックサムを説明した。このチェックサムの方法でも、特に文字データだけの場合は、意味のとれる形でデータを改竄することは非常に難しくなる。また、例えば、同じチェックサムを使う方法でも、文書を細かいブロックに区切って、ブロック毎のチェックサムを追加する方法や、文字を２次元に配置して、その縦方向と横方向のチェックサムを使うなどの方法で、セキュリティ強度を上げることができる。文書データ自体に図形データなどを含む場合の改竄防止のための特徴量を求めることは、かなり面倒ではあるが、暗号化の手法を用いれば実現することは可能である。しかし、真に重要な内容は文字データとして記述するようにすれば、補助的な図形データ等は特に特徴量を求める対象から外すようにしても、実用上は問題ない場合が多い。

【００４４】また、この例では、撹乱データとして、図形データの中で、実際に特徴量データを反映させる位置を示すデータを使用している。これを１６ビットとしたのは、簡単に説明するためであって、ビット数をもっと増やしても構わない。さらに、ランダムに変化するビットを加えることによって、図形データの変換手段を解読して偽造しようとする試みに対する防衛手段としてもよい。この撹乱データを固定として、図形データ変換手段に組み込めば、特に外部からは見えなくなるので、請求項１に記載した如く、特に撹乱データはないものとして扱う事もできる。また、この撹乱データを時間的に変更するなどの手段を講じれば、さらにセキュリティ強度が高まる。また、特徴量を反映させる位置を、もっと元の図形に似せて限定すれば、一見、自然にかすれたようなイメージとなり、特殊なデータを含んでいる事を意識させないようになる。元の図形データをもっと、多くのドットで構成した細かいイメージとすると、更に自然な印影が得られる。図形データの変更に関してはここでは黒白の反転を例に述べたが、中間階調を表現するデータを持たせて階調変化させることも可能である。また、色の情報を持たせて、色調の変化とすることもできる。

【００４５】次に西洋風のサインの例を示す。図３は、文書データが英語文書データ、図形データがベクトルデータである場合について本発明に係る書類承認、承認検証のやり方を示した図である。図３（Ａ）は、英語の文書の例を示し、図３（Ｂ）は、その文書を構成する文字をコード化したデータの集まりを表している。日本語文書の場合と同様なチェックサムを計算すると、文字数６１個、文字コードをすべて数値とみなして合算した合計が５６４６（１０進数）となり、これを２進数で表すと「０００１０１１０００００１１１０」が得られる。図３（Ｃ）に示すサインの図形情報は、いわゆるベクトル図形データ、もっといえば、インクデータといわれる線分の連なりからなるデータである。線分の連なりからなるデータは始点と終点のＸＹ座標の集まりからなるデータであるからベクトルデータであることは疑いがない

が、ここでは、線分データや、インクデータのみならず円や円弧、楕円等のデータをも含む情報、すなわち一般にＣＡＤで扱う図形情報を持ってベクトルデータとよぶこととする。図３（Ｄ）に示すように図形データの中から１６点を選んで、文書の特徴量を反映させるポイントとしている。印鑑の場合と同様にチェックサムの値を２進数で表現し、その各ビットの状態をそれぞれの点の位置に反映させている。ここでは、ビットが１の場合に右方向に３ポイントずらし、ビットが０の場合はそのままにしている。図３（Ｅ）は、データの特徴量を反映させたサインを示し、図３（Ｆ）は、文書データの特徴量が反映されて移動した点を示している。特徴量の表現方法が異なる以外は電子印鑑の例と同じである。ここで、図形が粗いのは説明のため違いが分かるように粗くしたのであり、実際はもっと細かく点をとっておき、そこから１ドットだけずらす、といったことをすれば、人間の肉眼による視認の上ではほとんど同じように見えるようにすることも可能である。図３（Ｇ）は、電子的に表現された文書とそれに付加されたサインとを示す図である。本発明にいうサインのデータは書類の承認者がその都度、署名動作を実行する性質のものではなく、一度限り署名の筆跡を電子データとして取得し、それを他人が偽って承認処理をするのに使われないように本人が厳重に保存、保持して用いる性質のものである。尤も他人が用いる場合はありえるが、それは変更を加えられた図形データから特徴量を再現するための参照用としてのみ用いることが許容されるような処置がとられるのが望ましい。

【００４６】図４は、本発明に係る電子押印セキュリティシステムを、パーソナルコンピュータ、ＣＲＴ装置、タブレット及び電子印鑑で構成した場合のハードウェア構成を示した図であり、図５は、本発明に係る電子押印セキュリティシステムを、パーソナルコンピュータ、平板型表示装置（例えば、液晶表示装置）を積層配置したタブレット及び電子印鑑で構成した場合のハードウェア構成を示した図である。これらはいずれも図６から図８までに示した電子押印セキュリティシステムを構成し得るハードウェア構成である。図６から図８までのシステムに共通な特徴は電子印鑑なる器具（タブレットの位置指示器としても機能する器具）の内部に基準印影データ（前述した基準図形データに該当するものであるが、印鑑の場合は図形は印影となるので、必要に応じて基準印影データとよぶことにする）を保持することとし、電子印鑑はタブレットに対して位置指示器としての役割のみならず情報送信の役割をも果たす点にある。位置指示器の内部に情報を保持し、タブレットに対し、位置の指示を行うのみならず、保持する情報を引き渡す機能を有するような座標入力装置に関しては、本願と同一の出願人が別途特許出願をしている。例えば、特許出願公開公報平成３年第１８９７１６号（特許願平成１年第３２７２

７６号「位置検出装置及びその位置指示器」）、特許出願公開公報平成７年第２００１３７号（特許願平成５年第３３５８０２号「位置検出装置及びその位置指示器」）、特許出願公開公報平成８年第１６３１１号（特許願平成６年第１４８１８３号「コンピュータシステム」）がある。

【００４７】特許出願公開公報平成３年第１８９７１６号に開示された技術に関して、簡単に説明する。前提となるのは、電磁気的に位置指示器とタブレットとが結合することによりコードレス（位置指示器とタブレットとがケーブルにより接続されない）タブレットを実現するものである。そのようなコードレスタブレットについては出願人は、多くの製品を世に出している。特開平３－１８９７１６では、そのようなコードレスタブレットの改良として、同調回路を有する位置指示器と、該位置指示器に対して電波を交互に送受することによりその指定位置の座標値を求めるタブレットとからなる位置検出装置において、位置指示器の同調回路に一定以上の電気的エネルギー及び所定のタイミング情報を含む誘導電圧を生起させ得る電波を送信する手段と、前記所定のタイミング情報に基づく特定のタイミングに位置指示器の同調回路より発生する電波の位相角又は周波数を検出する手段とをタブレットに設けるとともに、同調回路に生起した誘導電圧より各部を駆動するための電気的エネルギーを抽出する手段と、同調回路に生起した誘導電圧より所定のタイミング情報を抽出する手段と、該所定のタイミング情報に基づく特定のタイミングにスイッチ等の操作に基づいて同調回路の位相角又は周波数を変化させる手段とを位置指示器に設けたことを特徴とするものである。また、そのような位置検出装置であって、さらに、タブレット側に、位置指示器の同調回路に一定期間連続する誘導電圧及びこれに続く所定周期の間欠的な誘導電圧を生起させ得る電波を送信する手段を設けて、かつ、位置指示器側に同調回路に生起した一定期間連続する誘導電圧及びこれに続く所定周期の間欠的な誘導電圧を所定のタイミング情報として抽出する手段を設けることをも提案している。さらに、タブレット側に特定のタイミングに検出した位相角又は周波数の変化をコードに変換する手段を設け、かつ、位置指示器側にスイッチ等の操作に応じた特定のコードに従って同調回路の位相角又は周波数を変化させる手段を設けることをも提案している。

【００４８】特許出願公開公報平成７年第２００１３７号に開示された技術について簡単に説明する。コードレスタブレットの改良技術であることは同様である。この出願において出願人は、少なくとも２つの動作状態を有する位置指示器からその指示位置の座標値に対応する一定の空間分布を有する電磁波を発生し、これをタブレットで検出して該位置指示器による指示位置の座標値を求める位置検出装置において、位置指示器に、タブレット

側から送信される動作状態の設定命令を含む電磁波を受信する電磁波受信手段と、該受信した電磁波より動作状態の設定命令を抽出する命令抽出手段と、該動作状態の設定命令に従って動作状態を設定する動作設定手段とを設け、タブレットに、位置指示器に対する動作状態の設定命令を発生する命令発生手段と、該動作状態の設定命令を含む電磁波を位置指示器側へ送信する電磁波送信手段とを設けたことを特徴とする位置検出装置を提案した。また、指示位置の座標値に対応する一定の空間分布を有する電磁波を発生する電磁波発生手段と、該電磁波発生手段から発生する電磁波の強度特性または周波数特性もしくはこれらの特性の時間的変化を所定の制御情報に応じて制御する特性制御手段と、タブレット側から送信される動作状態の設定命令を含む電磁波を受信する電磁波受信手段と、該受信した電磁波より動作状態の設定命令を抽出する命令抽出手段と、該動作状態の設定命令に従って少なくとも２つの動作状態のいずれかに設定し、該設定された動作状態に基づく情報を前記所定の制御情報として入力可能とする動作設定手段とを備えた位置指示器と、位置指示器に対する動作状態の設定命令を発生する命令発生手段と、該動作状態の設定命令を含む電磁波を位置指示器側へ送信する電磁波送信手段と、位置指示器側から発生する一定の空間分布を有する電磁波を検出する電磁波検出手段と、該検出した電磁波より位置指示器による指示位置の座標値を求める座標検出手段と、前記検出した電磁波の強度特性または周波数特性もしくはこれらの特性の時間的変化を検出する特性検出手段と、該検出した電磁波の特性より情報を識別する情報識別手段とを備えたタブレットからなることを特徴とする位置検出装置をも提案した。さらに、指示位置の座標値に対応する一定の空間分布を有する電磁波を発生する電磁波発生手段と、該電磁波発生手段から発生する電磁波の強度特性または周波数特性もしくはこれらの特性の時間的変化を所定の制御情報に従って制御する特性制御手段と、少なくとも一つの指示器情報を発生する情報発生手段と、タブレット側から送信される指示器情報の要求命令を含む電磁波を受信する電磁波受信手段と、該受信した電磁波より指示器情報の要求命令を抽出する命令抽出手段と、該指示器情報の要求命令に従って前記指示器情報を前記所定の制御情報として設定する情報設定手段とを備えた位置指示器と、位置指示器に対する指示器情報の要求命令を発生する命令発生手段と、該指示器情報の要求命令を含む電磁波を位置指示器側へ送信する電磁波送信手段と、位置指示器側から発生する一定の空間分布を有する電磁波を検出する電磁波検出手段と、該検出した電磁波より位置指示器による指示位置の座標値を求める座標検出手段と、前記検出した電磁波の特性より指示器情報を識別する情報識別手段とを備えたタブレットとからなることを特徴とする位置検出装置をも提案した。指示位置の座標値に対応する一定の空間分布を有する電磁波を発生する電磁波発生手段と、該電磁波発生手段から発生する電磁波の強度特性または周波数特性もしくはこれらの特性の時間的変化を所定の制御情報に従って制御する特性制御手段と、複数種類の指示器情報をそれぞれ発生する複数種類の情報発生手段と、タブレット側から送信される所定の種類の指示器情報の要求命令を含む電磁波を受信する電磁波受信手段と、該受信した電磁波より所定の種類の指示器情報の要求命令を抽出する命令抽出手段と、該指示器情報の要求命令に従って前記複数種類の指示器情報のうちから該当する種類の指示器情報を選択して前記所定の制御情報として設定する情報設定手段とを備えた位置指示器と、位置指示器に対する所定の種類の指示器情報の要求命令を発生する命令発生手段と、該指示器情報の要求命令を含む電磁波を位置指示器側へ送信する電磁波送信手段と、位置指示器側から発生する一定の空間分布を有する電磁波を検出する電磁波検出手段と、該検出した電磁波より位置指示器による指示位置の座標値を求める座標検出手段と、前記検出した電磁波の強度特性または周波数特性もしくはこれらの特性の時間的変化を検出する特性検出手段と、該検出した電磁波の特性より所定の種類の指示器情報を識別する情報識別手段とを備えたタブレットとからなることを特徴とする位置検出装置をも提案した。さらに、これらの位置検出装置において、送信する電磁波の継続時間または休止時間により位置指示器側に対する命令を表すようになすことをも提案した。さらにまた、位置指示器の電磁波受信手段として共振回路を用いることを提案した。また、位置指示器の共振回路を電磁波発生手段として用いることをも提案した。また、位置指示器の特性制御手段として共振回路の共振特性を変えるようになすことをも提案した。共振回路に受信される電磁波から位置指示器の各部を駆動する電気的エネルギーを抽出する電源抽出手段を備えることをも提案した。

【００４９】特許出願公開公報平成８年第１６３１１号に開示された技術について簡単に説明する。この出願において出願人は、位置指示器より位置検出装置本体に対し位置情報以外の情報をも伝達可能な位置検出装置と、該位置検出装置を主たる入力デバイスとするソフトウェアを備えたコンピュータシステムにおいて、特定の位置指示器に特定のソフトウェアに対応した位置指示器であることを示す識別情報を発生する識別情報発生手段を設け、前記特定の位置指示器より発せられ位置検出装置本体を介して入力される識別情報から特定のソフトウェアを認識するソフトウェア認識手段と、前記特定の位置指示器の使用に伴って位置検出装置本体から出力される各種の情報を特定のソフトウェアのみに選択的に入力するソフトウェア選択手段とを備えたことを特徴とするコンピュータシステムを提案した。また、位置指示器より位置検出装置本体に対し位置情報以外の情報も伝達可能な位置検出装置と、該位置検出装置を主たる入力デバイス

とするソフトウェアとを備えたコンピュータシステムにおいて、特定の位置指示器に特定のソフトウェアに対応した位置指示器であることを示す識別情報を発生する識別情報発生手段を設け、前記特定の位置指示器より発せられ位置検出装置本体を介して入力される識別情報から特定のソフトウェアを認識するトフトウェア認識手段と、該特定のソフトウェアが既に起動されているか否かを判定する起動判定手段と、該判定の結果、起動されていなければ、該特定のソフトウェアを起動するソフトウェア起動手段とを備えたことを特徴とするコンピュータシステムをも提案した。さらに、位置指示器より位置検出装置本体に対し位置情報以外の情報も伝達可能な位置検出装置と、該位置検出装置を主たる入力デバイスとするソフトウェアとを備えたコンピュータシステムにおいて、特定の位置指示器に特定のソフトウェアに対応した位置指示器であることを示す識別情報を発生する識別情報発生手段を設け、前記特定の位置指示器より発せられ位置検出装置本体を介して入力される識別情報から特定のソフトウェアを認識するソフトウェア認識手段と、該特定のソフトウェアが既に起動されているか否かを判定する起動判定手段と、該判定の結果、起動されていなければ、該特定のソフトウェアを起動するソフトウェア起動手段と、前記特定の位置指示器の使用に伴って位置検出装置本体から出力される各種の情報を特定のソフトウェアのみに入力するソフトウェア選択手段とを備えたことを特徴とするコンピュータシステムをも提案した。さらに、上記のコンピュータシステムにおいて、特定の位置指示器が特定のソフトウェアに最適化された態様を有することを特徴とするコンピュータシステムを提案した。また、コードレスでかつ電池を電源とする位置指示器を備えた位置検出装置を用いることを特徴とする上記コンピュータシステムを提案した。さらにまた、コードレスでかつ共振回路を有する位置指示器を備えた位置検出装置を用いることを特徴とする上記コンピュータシステムをも提案した。コードレスでかつ共振回路を有し、該共振回路に発生するエネルギーを電源とする位置指示器を備えた位置検出装置を用いることを特徴とする上記コンピュータシステムをも提案した。

【００５０】これら３件の特許出願に開示された技術を持ってすれば、図６から図８までに描かれたセキュリティシステムを構成することが可能になる。図４及び図５に描いたタブレットは、これら３件に開示されたタブレットまたは位置検出装置と表現されたものに該当する。また、図４及び図５に描いた電子印鑑は、上記３件の特許出願において位置指示器と表現されたものに該当する。図６から図８における電子印鑑では基準図形データのセキュリティの問題を解決すべく、電子印鑑の筐体内部に基準図形データを保持することとしているのが第一の特徴である。図４及び図５に示した電子印鑑はタブレットとは何らのケーブルによる接続をもなされずに独立

の筐体により構成される。図４におけるパソコン、ＣＲＴ、タブレット間及び図５におけるパソコンと平板型表示装置の積層配置されたタブレットとはケーブル接続されるのが普通であるが、それを描くのを省略した。図４に示す構成例では電子印鑑をもって押印する場所はタブレット上であるがその印影が表示されるのはＣＲＴ装置上となる。図５に示す構成例では電子印鑑をもって押印する場所とその印影が表示される場所とが一致するのでより紙の書類に押印するのと近似した感覚で押印作業ができることとなる。位置検出装置を使うメリットとして、押印する位置に意味のある場合があることを指摘しておく。日本国において用いられる紙の文書であれば、役職によって、押印する位置は決まっている場合がある。その場合は、押すべき位置に自動的に押せるようにすれば、位置の指示は不要である。しかし、例えば、上司が不在のときに代理で印を押すときは、いつもとは違う欄に押す必要がある。そのような場合は押印位置を直接指示できるメリットが現れる。また、例えば、訂正印の場合、すなわち、訂正を欲する場所にその訂正を実行する主体が本人の同一性を確認するために押印する場合には、その押印位置に意味がある。これも位置検出装置を使うメリットになる。

【００５１】図６は、電子印鑑の筐体内部に基準印影データを保持することにより簡単なセキュリティ機能を実現した電子押印セキュリティシステムの機能ブロック図である。図６に示す実施例では、電子押印処理装置１０１には、位置検出部１４１及び情報通信装置１５１が設けられている点が、図１に示す電子押印または電子サイン処理装置１００と異なる点である。位置検出部１４１は、デジタイザタブレットと呼ばれることのある座標検出装置のうちの平板上のセンサを含む側の装置により主に構成される。座標検出装置は、一般に電子ペンや、カーソル（パック形状の位置指示器）等の位置指示器を平板上の座標検出領域に置いて、操作者がその位置指示器を動かすことにより座標（ＸＹ座標）をコンピュータに入力する装置である。電子印鑑３００は、そのような座標検出装置上の座標検出領域内の位置を示す位置指示部３１０を備えた位置指示器であり、かつ、内部に基準印影データを保持し、情報通信部３２０をも兼ね備えた器具である。このような電子印鑑３００を、内部にＣＰＵや、電池を備えたものとして構成して電子印鑑３００を電子押印装置１０１とはコードで接続されずに分離して設けることができるのは、図７等に示す実施例にあるように、比較的容易に構成し得る。本願と同一出願人が既に出願し、提案した上述の３件の技術を用いれば、ＣＰＵや電池を電子印鑑３００の筐体内部に設けなくとも図６に示す電子印鑑３００を構成することができる。

【００５２】ごく簡単に、上述の３件の技術を振り返ると、特開平３－１８９７１６では、共振回路を有する位置指示器とタブレットとの間で電磁結合をするコードレ

スタブレットにおいて、タブレットからのタイミング情報を位置指示器が受けることによりコード情報を位相角または周波数の変化としてタブレット側に返してタブレットはそれを検出して位置指示器のコード情報を取得し得るものを開示した。この位置指示器の筐体内部に不揮発性メモリを設けて、基準印影データ（＋撹乱データ）を保持すれば、図６に示す電子印鑑３００の基本的な構成が実現できる。さらに、特開平７－２００１３７では、タブレットからコードレスの位置指示器に対し各種の命令を送ってその動作を制御可能な位置検出装置及びその位置指示器を提案し、また、必要な時のみ指示器情報を位置指示器からタブレットへ伝達可能な位置検出装置及びその位置指示器を提案し、さらに、位置指示器に複数の情報が蓄えられている場合に、必要な種類の指示器情報のみを位置指示器からタブレットへ伝達可能な位置検出装置及びその位置指示器を提案した。従って、電子印鑑３００は、電子押印処理装置１０１が必要な時のみ必要なデータを引き渡すことができる。また、さらに、特開平８－１６３１１では、位置指示器側にコンピュータ側のソフトウェアを認識し、必要があれば、それを起動し、また、特定のソフトウェアのみに選択的に入力することができる機能を持たせることを提案した。この技術によれば、電子印鑑３００を電子押印処理装置１０１を構成する位置検出部１４１及び情報通信装置１５１に近づけると、電子押印処理装置１０１を構成するコンピュータがそれまで他の処理（例えば、ワードプロセッサのテキスト入力処理）を実行していた場合でも、自動的に電子押印処理のソフトウェアが起動して当該コンピュータが電子押印処理装置１０１として機能することを担保できる。また、電子押印処理のソフトウェア以外のソフトウェアに対しては基準印影データ（＋撹乱データ）Ｄ００２の引渡しを拒否することが可能であるため、秘密とすべきこの種のデータのセキュリティ上都合がよい。

【００５３】図６に示した実施例が、図１に示した基本構成と異なるもう一つの点がある。電子印鑑３００の情報送信部３２０から電子押印の検証処理装置２０１の情報通信装置２５１への矢印の意味するものである。情報通信装置２５１と情報送信部３２０との間は、例えば電磁結合により情報のやりとりが可能である。即ち、上述の３件の特許出願に開示された技術によりそれを構成できる。ここでは、位置指示及び位置検出の機能は捨象できるから、情報送信部３２０側の共振回路と情報通信装置２５１側のアンテナ（ループコイル）との間で電磁結合がなされ、その波形の変化の情報にあるタイミングでコード情報を載せることによって情報のやりとりがなされ得る。また、電子押印の検証処理装置２０１は、通常、汎用パソコンによって構成されるが、そのソフトウェアが押印の検証処理ソフトウェアである場合にのみ基準印影データ（＋撹乱データ）Ｄ００２を参照し得るようにすべく電子印鑑３００が情報通信装置２５１に近づいたときにのみ検証処理ソフトウェアまたはそのための基準印影データ参照ソフトウェアが動作するように構成することも上述の技術により可能である。

【００５４】さらに、電子押印の検証処理装置２０１の検証ソフトウェアは、情報通信装置２５１を介して参照した基準印影データ（＋撹乱データ）Ｄ００２を特徴量再現部２２０にて特徴量を再現するための参照用にのみ用い、不必要な記憶、保持はしないことがセキュリティ上、望ましい。電子押印の検証処理装置２０１上の記憶装置に何らかの形で基準印影データ（＋撹乱データ）Ｄ００２を残しては、当該装置を構成するコンピュータ（パソコン）の操作者、使用者が他人の印影を用い文書を偽造するおそれがあるからである。

【００５５】斯かるセキュリティ上の見地から図６における電子印鑑３００は、押印処理を実行する者が一つだけ保管し、厳重に管理する性質のものであり、複数あることは好ましくない。この点においても図１に示す基本構成が押印者のコンピュータとネットワークサーバとの二箇所に基準印影データ（＋撹乱データ）をおく必要があるのと異なる点である。図６における電子印鑑３００は、たった一つのものであり、検証処理の際には押印者本人が電子押印の検証処理装置２０１にまで出向く必要のあるものである。そもそも、本願に係る電子押印は、図１１（Ｂ）に示す従来例のＰＧＰシグネチャと異なり、常に検証を必要とするものではなく、一応は目視により相当の確からしさを確認できるものであって、疑義の生じたときのみ検証を必要とするものであるから、図６に示す電子印鑑を用いたセキュリティシステムであっても、簡単な電子書類のセキュリティシステムは実現できたといえる。なお、図６における実施例の特徴をもう一つつけ加えると、電子押印処理装置１０１の中の印影データ押印部１３１では、変更の加えられた印影データを印影データ変更手段１２１から受け取るとともに、押印位置の情報を位置検出部１４１から得て文書データＤ００１の然るべき位置（押印者が欲する位置）に印影データを付加することができる。このようにして押印された電子文書Ｄ００３が生成される点が、図１に示す基本構成と異なる。電子印鑑３００が位置指示器でもあるゆえんである。

【００５６】図６に示すセキュリティシステムに限界があるとすれば、基準印影データ（＋撹乱データ）Ｄ００２がたとえ一時的にせよ、電子押印装置１０１または電子押印の検証処理装置２０１に引き渡される点にある。この種のシステムは複数人のグループの人間の間で適用されるが、その複数人の中の一人に個人情報を盗んで悪用しようとする者が出たときにその者がソフトウェアを書き換えて本来個人情報であるべき基準印影データ（＋撹乱データ）Ｄ００２等にアクセスして不当にそれを取得する可能性を全くなしとし得ないのが図６に示す実施

例の限界といえる。

【００５７】図７は、電子印鑑の内部で印影データ変更、印影データー致判定等の処理を行うことにより高度なセキュリティ機能を実現した電子押印セキュリティシステムの機能ブロック図である。図７に示す実施例では、電子印鑑３０１は、内部にＣＰＵや電池を備えることにより一個の独立したコンピュータとして働くものである。特徴量抽出部１１０及び印影データ変更手段１２１は図６の実施例では電子押印処理装置１０１の内部に設けられていたが、図７では、電子印鑑３００の筐体内部に設けられる。また、図７の印影データー致判定部２３１は、図６に示す実施例の電子押印の検証処理装置２０１内の特徴量一定判定部２３０に相当するものである。

【００５８】図７に示す実施例に関して、処理の流れにしたがって、説明する。電子押印処理装置１０２は汎用コンピュータに必要な電子書類セキュリティのためのソフトウェアが組み込まれたものであり、その入力機器としてデジタイザタブレット（座標入力装置）が接続されている。当該タブレットは電子印鑑３０１を位置指示器として用いるとともに電子印鑑３０１との間で情報通信機能をも有するものである。電子印鑑３０１と電子押印処理装置１０２側のデジタイザタブレットとは例えば、電磁気的な結合をすることにより電気的な非接触状態でも情報のやり取りが可能である。電子押印処理装置１０２に文書データＤ００１が読み込まれているときに電子印鑑３０１が電子押印処理装置１０２のデジタイザタブレットに近づくと電子押印処理装置１０２は文書データＤ００１を情報通信装置１５２を介して電子印鑑３０１に引き渡す。電子印鑑３０１側の情報通信部３２１は、文書データＤ００１を受け取ってその特徴量を抽出すべくそのデータを電子印鑑３０１内の特徴量抽出部１１０に引き渡す。図７の電子印鑑３０１内の特徴量抽出部１１０は、図１における電子押印または電子サイン処理装置１００内の特徴量抽出部１１０、図６における電子押印処理装置１０１内の特徴量抽出部１１０と同様の処理を実行して文書データ００１の特徴量を抽出する。抽出された特徴量は図７の電子印鑑３０１ないの印影データ変更手段１２１に引き渡される。

【００５９】図７の電子印鑑３０１内の印影データ変更手段１２１は、基準印影データ（＋撹乱データ）Ｄ００２に対して特徴量に応じた変更を加え、変更後の印影データを情報通信部３２１に返す。図７の実施例にあっては、基準印影データ（＋撹乱データ）Ｄ００２は、電子印鑑３０１内の記憶手段に保持されるものの、当該データにアクセス可能な手段は印影データ変更手段１２１のみであり、かつ、印影データ変更手段１２１はＤ００２をそのまま外部に出力することはせず、変更を加えた印影データのみを情報通信部３２１に返すこととするのが望ましい。図７の実施例はＤ００２のデータが生のまま

外部に出ることを防ぐことによりセキュリティ強度を高めることを目的とした実施例だからである。図７に示す電子印鑑３０１内の印影データ変更手段１２１の実行する処理内容は、図１に示す電子押印または電子サイン処理装置１００内の図形データ変更手段１２０、図６に示す電子押印処理装置１０１内の印影データ変更手段１２１の実行する処理内容と同様である。

【００６０】電子印鑑３０１内の情報通信部３２１は、変更を加えられた印影データを受け取るとそれを、電子押印処理装置１０２内の情報通信装置１５２に返す。電子押印処理装置１０２内の情報通信装置１５２は当該印影データを受け取ると電子押印処理装置１０２内の印影データ押印部１３１に送る。一方、電子押印処理装置１０２内の位置検出部１４１は、電子印鑑３０１の位置指示部３１０がタブレット上のどの位置を指示しているかを検出し、当該位置に関する座標データを押印位置として印影データ押印部１３１に引き渡す。印影データ押印部１３１は、電子書類のデータである文書データＤ００１に対して位置検出部１４１から送られた押印位置に情報通信装置１５２から得られた印影データを押印する処理を実行して押印された電子文書００３を生成する。押印された電子文書Ｄ００３は、文書データと文書データの特徴量により変形された印影データを組み合わせたものであり、このデータの生成により電子押印処理装置１０２による押印処理が完結される。

【００６１】次に、図７に示す電子押印の検証処理について説明する。既に述べたように変形された印影データは押印者本人を示す紋章、記章等の図形であって、その図形の外観形状に特徴を有するものであり、変更を加えた印影は見た目には基準印影とほぼ同一のものであるから、押印された電子文書が、例えば社内ＬＡＮ（ローカルエリアネットワーク）で転々としたとしてもその都度電子的な検証をする必要のあるものではない。最終的な決定をする必要がある場合等に電子押印の検証処理装置２０２の処理がなされる。この検証処理は押印の際に用いたのと同じ固有の電子印鑑３０１を電子押印の検証処理装置２０２の近くに持ってくることによってなされる。

【００６２】すなわち、検証の必要が生じた時には、押印された電子文書Ｄ００３は、電子押印の検証処理装置２０２内の情報通信装置２５２により電子印鑑３０１内の情報通信部３２１に送られる。情報通信部３２１は、押印された電子文書Ｄ００３を文書データと印影データとに分離して、文書データは電子印鑑３０１内の特徴量抽出部１１０に、印影データは電子印鑑３０１内の印影データー致判定部２３１に送る。尤も押印された電子文書Ｄ００３を文書データと印影データとに分離する処理は（特にそれが複雑な処理である場合には）電子押印の検証処理装置２０２側で行うことが望ましい。セキュリティ上の問題も生じないからである。

【００６３】電子印鑑３０１内の情報通信部３２１から電子印鑑３０１の特徴量抽出部１１０に送られた文書データは、当初の文書データＤ００１と同じもののはずである。電子印鑑の特徴量抽出部１１０は、当該文書データから特徴量を再び抽出する。再びという意味は押印処理の際に一度行った処理と同一の処理を今度は電子押印の検証処理装置２０２の情報通信装置２５２から送られた文書データに対して実行するという意味である。抽出された特徴量は、電子印鑑３０１内の印影データ変更手段１２１に送られる。印影データ変更手段１２１は、基準印影データ（＋撹乱データ）Ｄ００２を取得し、それに対して特徴量に応じた変更を加える。変更を加えられた印影データは電子印鑑３０１内の印影データ変更手段１２１から電子印鑑３０１内の印影データー致判定部２３１に送られる。電子印鑑内の印影データー致判定部２３１は、情報通信部３２１から受け取った印影データと印影データ変更手段１２１から受け取った印影データとを比較して一致するか否かを判定する。電子印鑑３０１内の印影データー致判定部２３１は、二つの印影データが一致する場合には、文書データＤ００３が真正なものとの判定結果を情報通信部３２１に送り、不一致の場合には真正なものではないとの判定結果を情報通信部３２１に送る。電子印鑑３０１内の情報通信部３２１は、電子押印の検証処理装置２０２内の情報通信装置２５２に当該判定結果を送り、電子押印の検証処理装置２０２は、当該結果を出力する。このようにして押印された電子文書Ｄ００３の検証処理が完結する。

【００６４】図７における実施例では、検証処理のために特徴量の一致を判定せずに印影データの一致を判定したのは、電子印鑑３０１内には既に特徴量抽出部１１０が存在するから、それのほかに図１や図６のような特徴量再現部２２０を重ねて設けるのは無益だからである。それに対して、図１や図６では印影データの一致を判定せずに特徴量の一致を判定したのは、セキュリティ上の理由による。すなわち、図１の電子押印または電子サイン処理装置１００内または図６の電子押印処理装置１０１内の特徴量抽出部１１０及び図形データ変更手段１２０または印影データ変更手段１２１の処理を、図１の電子押印または電子サインの検証処理装置２００または図６の電子押印の検証処理装置２０１において実行したとすると、検証処理装置側で押印処理装置と同様の処理が実行可能となるので、他人になりすまして押印を実行する不正処理の横行を許容する結果となり、セキュリティ上問題だからである。そこで、図１や、図６の実施例では、図形データ変更や印影データ変更の逆変換の機能である特徴量再現という機能のみを検証処理装置側に持たせて、セキュリティの問題に対する措置を講じたものである。

【００６４】それに対して、図７の実施例では、電子印鑑３０１は押印者本人のみが一個のみ所有し、保管するものであるという前提からセキュリティに関するこの問題をクリアできるため印影データの一致判定をすることにより合理化を図った。

【００６５】図８は、電子印鑑内における印影データ変更を秘密鍵データに基づく文書データの暗号化処理に基づいて行うことによりさらに高度なセキュリティ機能を実現した電子押印セキュリティシステムの機能ブロック図である。秘密鍵データに基づく文書データの暗号化処理とは、前述した公開鍵暗号化方式に基づいて押印者（署名者）本人が所持、保管する秘密鍵データに基づいて文書データを暗号化（撹乱）する処理のことである。

【００６６】図８における実施例が、図７における実施例と異なる点を列挙すると、電子印鑑３０２内に秘密鍵データＤ００４を格納した点、図７の特徴量抽出部１１０に代えて暗号化処理部１１１を設けた点、電子印鑑３０２内では検証処理における一致判定を行わずに電子押印の検証処理装置２０３内で一致判定を文書データー致判定部２３２にて行うこととした点、公開情報格納装置４００を設けて基準印影データＤ２０２と公開鍵データＤ００５とを格納することとした点、電子押印の検証処理装置２０３内に暗号化された文書データの抽出手段２２１と復号化処理部２２２を設けた点、などである。

【００６７】図８における実施例を処理の流れにしたがって説明する。電子押印処理装置１０２の構成は図７における実施例と同一であり、同様の処理を実行する。電子押印処理装置１０２が文書データＤ００１を扱っている状態で、電子印鑑３０２の位置指示部３１０を電子押印処理装置１０２の位置検出部１４１に近づけ、電子印鑑３０２の情報通信部３２２を電子押印処理装置１０２の情報通信装置１５２に近づけると、電子押印処理装置１０２は、文書データＤ００１を情報通信装置１５２を介して電子印鑑３０２の情報通信部３２２に送る。電子印鑑３０２の情報通信部３２２は、当該文書データＤ００１は、情報通信部３２２から暗号化処理部１１１に送られる。暗号化処理部１１１は、電子印鑑３０２内に格納された秘密鍵データＤ００４を取得し、該秘密鍵データＤ００４に基づいて文書データＤ００１を暗号化する。暗号化された文書データは、暗号化処理部１１１から印影データ変更手段１２２へ送られる。

【００６８】印影データ変更手段１２２は、電子印鑑３０２内に予め格納された基準印影データＤ００２を取得し、当該基準印影データＤ００２に対して、暗号化処理部１１１の出力である暗号化された文書データに基づいて（当該暗号化された文書データの特徴を反映して）、変形、修正等の変更を加える。変更処理は、図１の実施例における図形データ変更手段１２０、図６または図７の実施例における印影データ変更手段１２１と同様の処理となる。変更された印影データは情報通信部３２２に送られる。情報通信部３２２は、変更された印影データを電子押印装置１０２の情報通信装置１５２に送る。電

子押印装置１０２の情報通信装置１５２は、当該変更された印影データを電子押印処理装置１０２の印影データ押印部１３１に送る。

【００６９】一方、電子印鑑３０２の位置指示部３１０は、電子印鑑３０２の置かれた位置を電子押印処理装置１０２の位置検出部１４１に対して指示し、電子押印処理装置１０２の位置検出部１４１は、電子印鑑３０２の位置指示部３１０が指示する位置を検出し、その押印位置の情報（座標情報）を電子押印処理装置１０２の印影データ押印部１３１に送る。電子押印処理装置１０２の印影データ押印部１３１は、情報通信装置１５２から得られた印影データを位置検出部１４１から得られた押印位置の情報により文書データＤ００１に付加して押印された電子文書Ｄ００３を出力する。このようにして押印済み電子文書が生成される。

【００７０】押印済み電子文書の検証処理をする必要が生じた場合には、電子押印の検証処理装置２０３が検証処理を実行する。図７における実施例では一致判定を電子印鑑３０１内において実行したが、図８における実施例では一致判定は電子押印の検証処理装置２０３が実行する点が異なる点のうちの一つである。また、図８における実施例では、公開情報格納装置４００が設けられ、その装置内に格納された基準印影データＤ００２及び公開鍵データＤ００５を用いて電子押印の検証処理装置２０３が検証処理を実行する点も異なる点である。この実施例において基準印影データＤ００２を公開情報とできるのは、たとえ悪意の者があってもこれのみでは電子印鑑の所持者本人を詐称することはできず、基準印影データＤ００２と秘密鍵データＤ００４との組み合わせによってのみ押印が可能だからである。

【００７１】押印済み電子文書の検証処理の流れを図８を参照しつつ説明する。まず電子押印の検証処理装置２０３は、押印された電子文書（押印済み電子文書）Ｄ００３を文書データと印影データとに分離する。この分離は、通常は単に付加されたものを分けるに過ぎない。分離された文書データは当初の平文である文書データＤ００１と同一のもののはずである。この文書データは文書データ一致判定部２３２に送られる。一方、分離された印影データは暗号化された文書データの抽出手段２２１に送られる。暗号化された文書データの抽出手段２２１は、公開情報格納装置400に格納された基準印影データＤ００２を参照して、印影データ変更の元となった暗号化されている文書データを抽出する。この抽出処理は電子印鑑３０２の印影データ変更手段１２２が実行する変更処理の逆の変換をする処理である。暗号化された文書データの抽出手段２２１の出力、すなわち暗号化されている文書データは、復号化処理部２２２に送られる。復号化処理部２２２は、公開情報格納装置４００に格納された公開鍵データＤ００５を用いて、暗号化されている文書データの復号化処理を実行する。その出力である復

号化された文書データは、文書データー致判定部２３２に送られる。文書データー致判定部２３２は、押印された電子文書Ｄ００３から分離された文書データと復号化処理部２２２により復号化された文書データとを比較して一致するか否かを判定する。そして、一致する場合には、押印済み電子文書Ｄ００３の押印を真正なものと判定結果を出力し、一致しない場合には押印済み電子文書Ｄ００３の押印を真正ではないと判定結果を出力する。

【００７２】図８に示す実施例では、公開情報格納装置４００に格納された基準印影データＤ００２及び公開鍵データＤ００５に基づいて検証処理を実行している。この点において、図７に示す実施例が電子印鑑３０１にて一致判定を実行するのと大きく異なっている。従って、図８の実施例では図７に比べて検証処理が身近なものとなっているといえる。図７では、一個しか存在しない電子印鑑３０１を前提とするため検証処理がおいそれとはできないのに対し、図８の実施例では公開情報格納装置にはなんびともアクセス可能だからである。

【００７３】図９は、本発明の基本構成に秘密鍵による暗号化及び公開鍵による復号化を加味した実施例を示す機能ブロック図である。図９に示す実施例を図１に示す本発明の基本構成と異なる点が２点ある。第一に、電子押印または電子サイン処理装置１０３において、文書データの特徴量を抽出した後、その特徴量そのものに基づいて図形データ変更処理を実行するのではなく、秘密鍵情報Ｄ００４により暗号化処理を施してからその結果に基づいて図形データ変更を実行すべく、暗号化処理手段１６０を設けた点である。第二に、電子押印または電子サインの検証処理装置２０３において、特徴量の再現をするのに図形データ解析処理と公開鍵情報Ｄ００５による復号化処理との２段階によりなしている点である。図１に示す基本構成で、出願人は、従来の電子シグネチャに代わるものとして図形データを用いた電子押印、電子署名の概念を提案したが、従来の秘密鍵、公開鍵による暗号化、復号化と組み合わせることによりさらにセキュリティ強度の高いシステムを構築できることを指摘すべく、図９に示す実施例を提案する。

【００７４】図９に示す実施例を図６から図８までの実施例に比較すると、最も大きな違いは位置指示部、及び位置検出部の捨象されている点である。図６から図８までにあっては、デジタイザタブレットの存在の有用性を指摘したが、図１の基本構成に位置検出の要素を加味しない場合であっても、秘密鍵、公開鍵による暗号化、復号化の要素を加味することが有用であることを指摘すべく提案するものである。

【００７５】図９に示す実施例が図１と共通する点に関しては図１と同一の符号を付している。共通する部分については前述したものと同様であるので、説明を省略する。

【００７６】図１０は、秘密鍵による暗号化処理と分離

可能なユニットにて実行する実施例を示す機能ブロック図である。図１０に示す実施例が図９の実施例と異なるのは、２点ある。第一に、暗号化処理部１６０を、電子押印または電子サイン処理装置１０４から分離して携帯可能なユニット５００内に設けて、そのユニット内部に秘密鍵情報Ｄ００４を格納した点である。第二に、図形データＤ００２と、公開鍵情報Ｄ００５とを公開情報サーバ４００内に格納した点である。

【００７７】秘密鍵情報Ｄ００４を分離して携帯可能なユニット５００内に格納することにより、該情報が他人に盗まれる危険が減り、セキュリティ強度を高めることが出きる。即ち、図１０に示す実施例では、秘密鍵情報は生のまま当該ユニットの外に出ることがない。秘密鍵情報の管理者は、このユニットを身につけて持ち歩くことにより、他人に使用される危険を回避できる。

【００７８】電子押印または電子サイン処理装置１０４と分離して携帯可能なユニット５００との間の情報のやりとりは、図７や図８に示した電子押印処理装置１０２と電子印鑑３０１、３０２との間の情報のやりとりと同様の方法、例えば電磁気的な結合による非接触の通信方法が可能である。分離して携帯可能なユニット５００は具体的にはＩＣカードのようなものとして構成することができる。図１０に示す実施例では当該ユニット内で暗号化処理を実行するので必要なＣＰＵを備えることになる。

【００７９】公開情報サーバ４００に図形データＤ００２、公開鍵情報Ｄ００５を格納することによりネットワークによる本システムの運用に適したものとなる。

【００８０】

【発明の効果】このようにして、電子印鑑や電子サインを施すことで、紙の書類に押印やサインにより決済を与えるのと同様の感覚で、電子的に決済や承認の可能なシステムを構築することができるようになった。ＯＡ（オフィスオートメーション）への効用が大きい。

【図面の簡単な説明】

【図１】　本発明に係る電子書類セキュリティシステム、電子押印セキュリティシステムまたは電子署名セキュリティシステムの基本構成を示す機能ブロック図

【図２】　文書データが日本語文書データ、図形データがビットマップデータである場合について本発明に係る書類承認、承認検証のやり方を示した図

【図３】　文書データが英語文書データ、図形データがベクトルデータである場合について本発明に係る書類承認、承認検証のやり方を示した図

【図４】　本発明に係る電子押印セキュリティシステムを、パーソナルコンピュータ、ＣＲＴ装置、タブレット及び電子印鑑で構成した場合のハードウェア構成を示した図

【図５】　本発明に係る電子押印セキュリティシステムを、パーソナルコンピュータ、平板型表示装置を積層配

置したタブレット及び電子印鑑で構成した場合のハードウェア構成を示した図

【図６】　電子印鑑の筐体内部に基準印影データを保持することにより簡単なセキュリティ機能を有する電子押印セキュリティシステムの機能ブロック図

【図７】　電子印鑑の内部で印影データ変更、印影データー致判定等の処理を行うことにより高度なセキュリティ機能を実現した電子押印セキュリティシステムの機能ブロック図

【図８】　電子印鑑内における印影データ変更を秘密鍵データに基づく文書データの暗号化処理に基づいて行うことによりさらに高度なセキュリティ機能を実現した電子押印セキュリティシステムの機能ブロック図

【図９】　本発明の基本構成に秘密鍵による暗号化及び公開鍵による復号化を加味した実施例を示す機能ブロック図

【図１０】　秘密鍵による暗号化処理を分離可能なユニットにて実行する実施例を示す機能ブロック図

【図１１】　従来例の電子署名を示す図

【符号の説明】

１００、１０３、１０４　電子押印又は電子サイン処理装置（電子書類承認操作装置）

１０１、１０２　電子押印処理装置

１１０　特徴量抽出部

１１１、１６０　暗号化処理部

１２０　図形データ変更手段

１２１、１２２　印影データ変更手段

１３１　印影データ押印部

１４１　位置検出部

１５１、１５２　情報通信装置

Ｄ００１　文書データ

Ｄ００２　図形データ（＋撹乱データ）

Ｄ００３　文書データ＋文書データの特徴量により変形された図形データ

Ｄ００４　秘密鍵データ

Ｄ００５　公開鍵データ

２００　電子押印又は電子サイン検証処理装置（電子書類承認検証装置）

２０１、２０２　電子押印の検証処理装置

２１０　特徴量抽出部

２２０　特徴量再現部

２２１　暗号化された文書データの抽出手段

２２２、２６０　復号化処理部

２２３　図形解析手段

２３０　特徴量一致判定部

２３１　印影データー致判定部

２３２　文書データー致判定部

２５１、２５２　情報通信装置

３００、３０１、３０２　電子印鑑

３１０　位置指示部

35

３２０、３２１、３２２　情報送信部

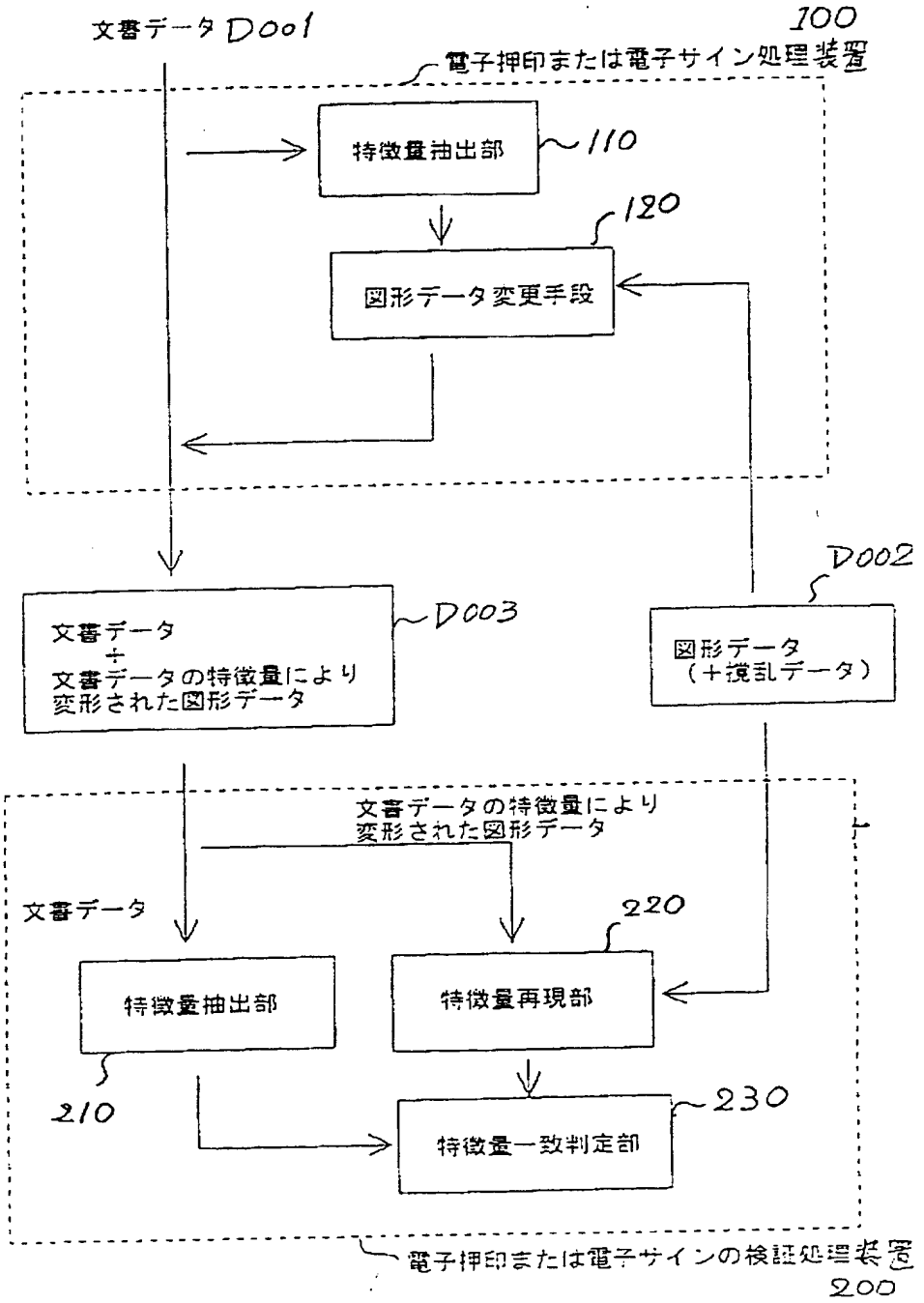
３３０　暗号化処理部

36

４００　公開情報格納装置

５００　分離して携帯可能なユニット

【図１】



【図２】

(A)

稟議書
新製品の製品化を提案します。
この製品で新しい市場を開拓します。
御決済をお願いします。

(B)

226	103	139	99	143	145	13	10	144	86
144	187	149	105	130	204	143	164	149	105
137	187	130	240	146	241	136	196	130	181
130	220	130	183	129	66	13	10	130	177
130	204	144	187	149	105	130	197	144	86
130	181	130	162	142	115	143	234	130	240
138	74	145	241	130	181	130	220	130	183
129	66	13	10	140	228	140	136	141	207
130	240	130	168	138	232	130	132	130	181
130	220	130	183	129	66				

(C)

(D)

(E)

(F)

(G)

稟議書
新製品の製品化を提案します。
この製品で新しい市場を開拓します。
御決済をお願いします。

【図３】

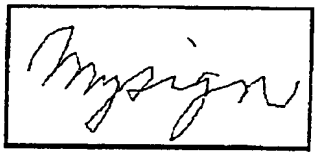
(A)

This is the very important document.
Never change this text.

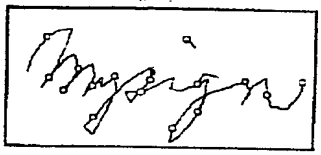
(B)

84	104	105	115	32	105	115	32	116	104
101	32	118	101	114	121	32	105	109	112
111	114	116	97	110	116	32	100	111	99
117	109	101	110	116	46	13	10	78	101
118	101	114	32	99	104	97	110	103	101
32	116	104	115	32	116	101	120	116	46

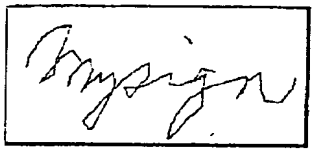
(C)



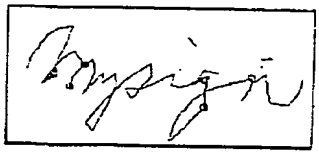
(D)



(E)



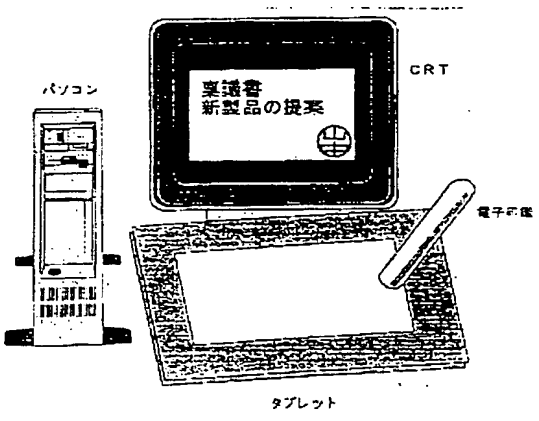
(F)



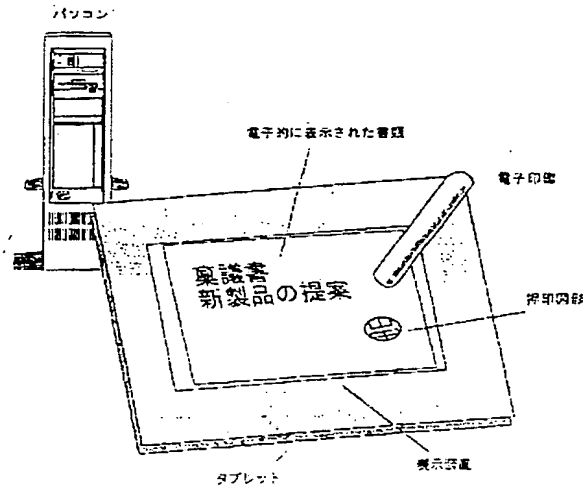
(G)

This is the very important document.
Never change this text.

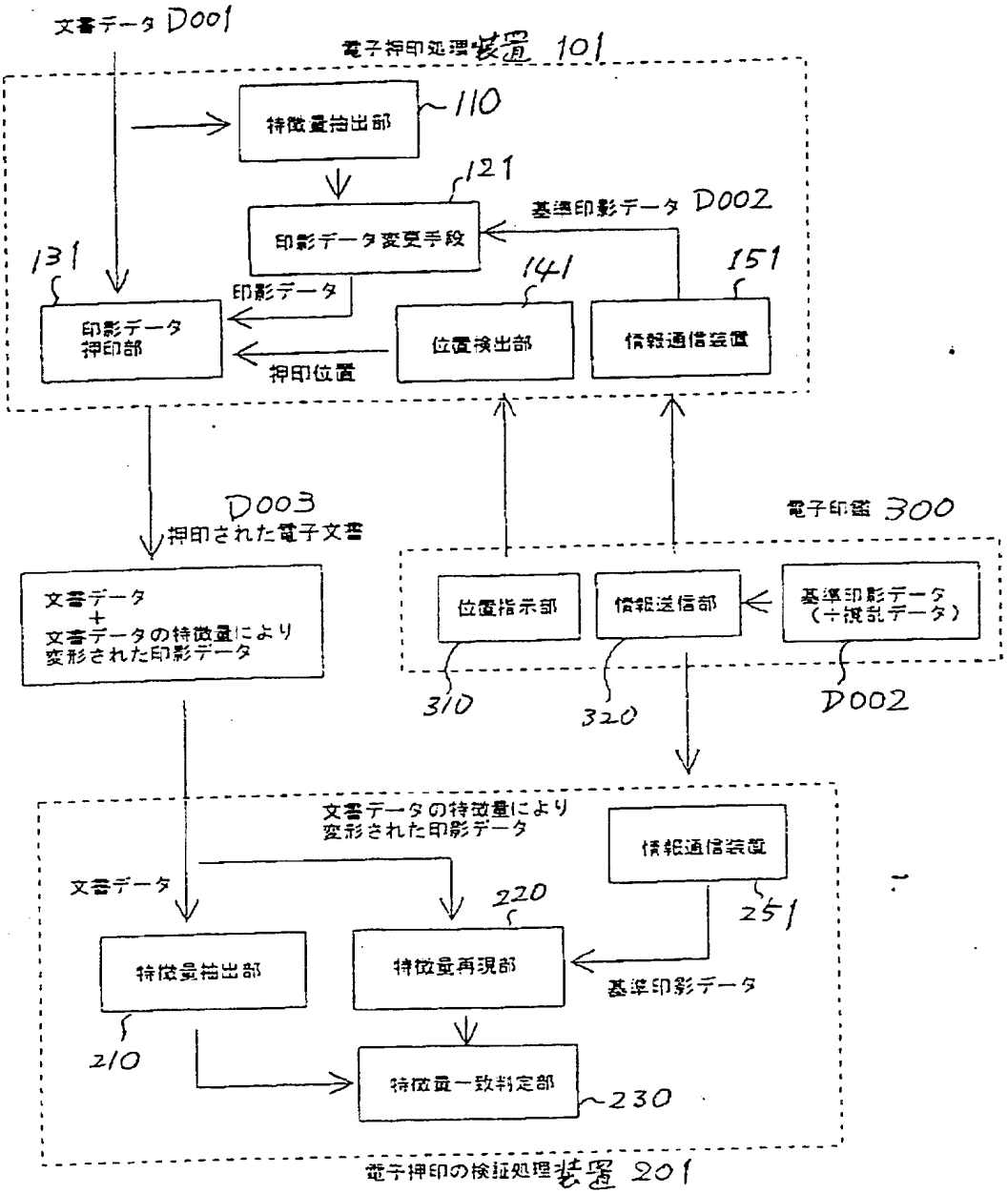
【図４】



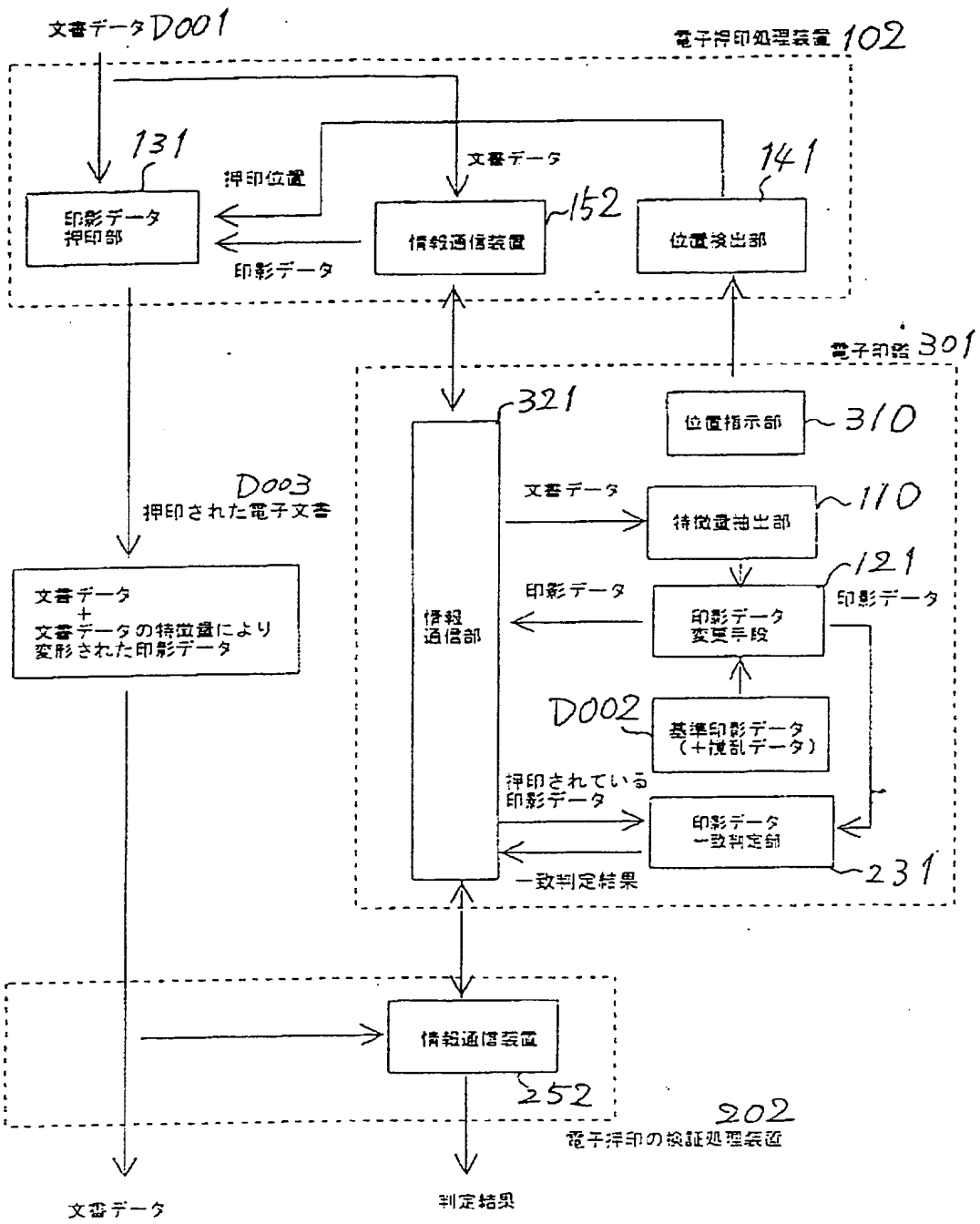
【図５】



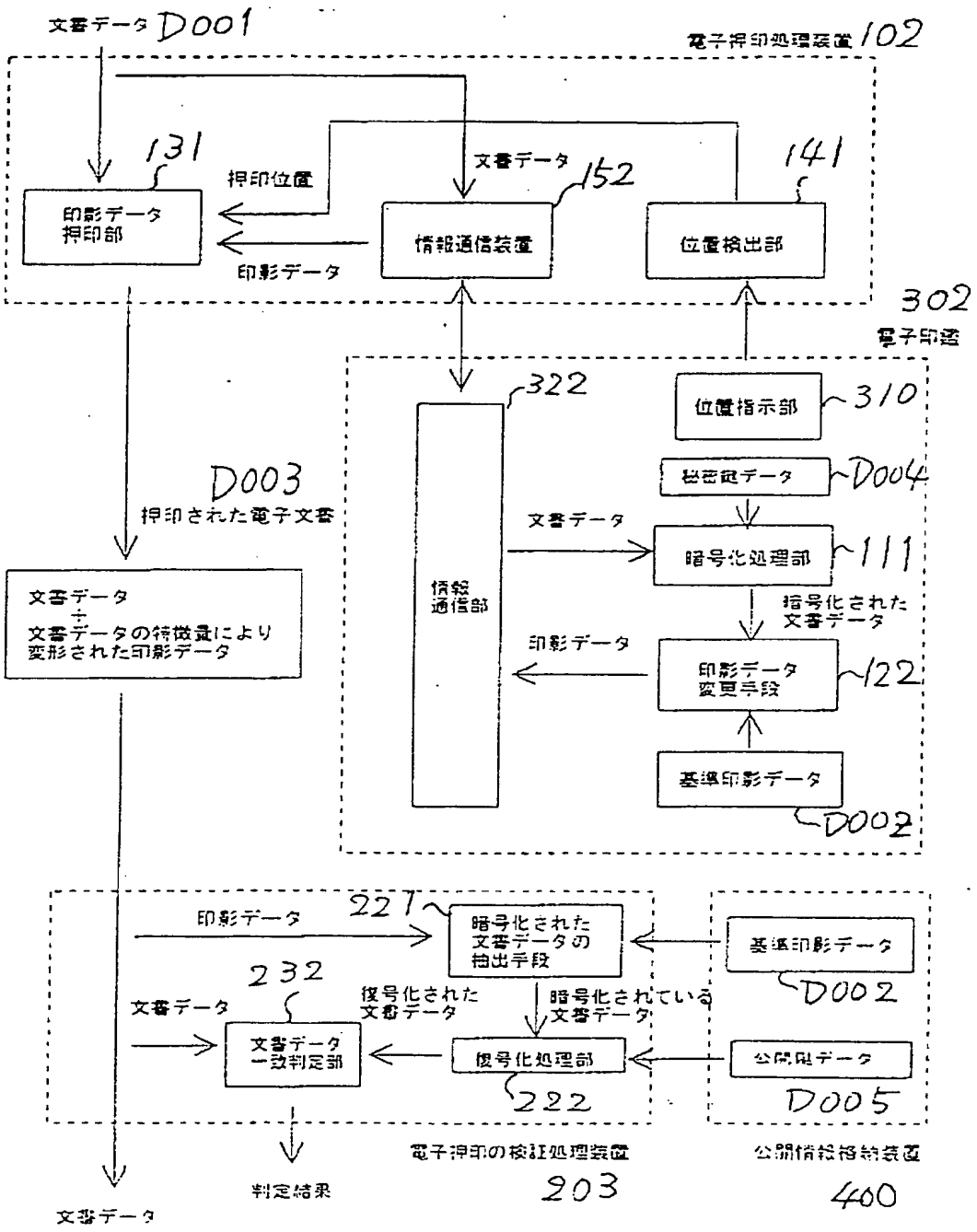
【図6】


文書データ D001
電子押印処理装置 101
特徴量抽出部
110
121
印影データ変更手段
基準印影データ D002
131
印影データ
押印部
印影データ
141
位置検出部
151
情報通信装置
押印位置
D003
押印された電子文書
文書データ
＋
文書データの特徴量により
変形された印影データ
電子印鑑 300
位置指示部
情報送信部
基準印影データ
（十規乱データ）
310
320
D002
文書データの特徴量により
変形された印影データ
情報通信装置
251
文書データ
220
特徴量抽出部
特徴量再現部
基準印影データ
210
特徴量一致判定部
230
電子押印の検証処理装置 201

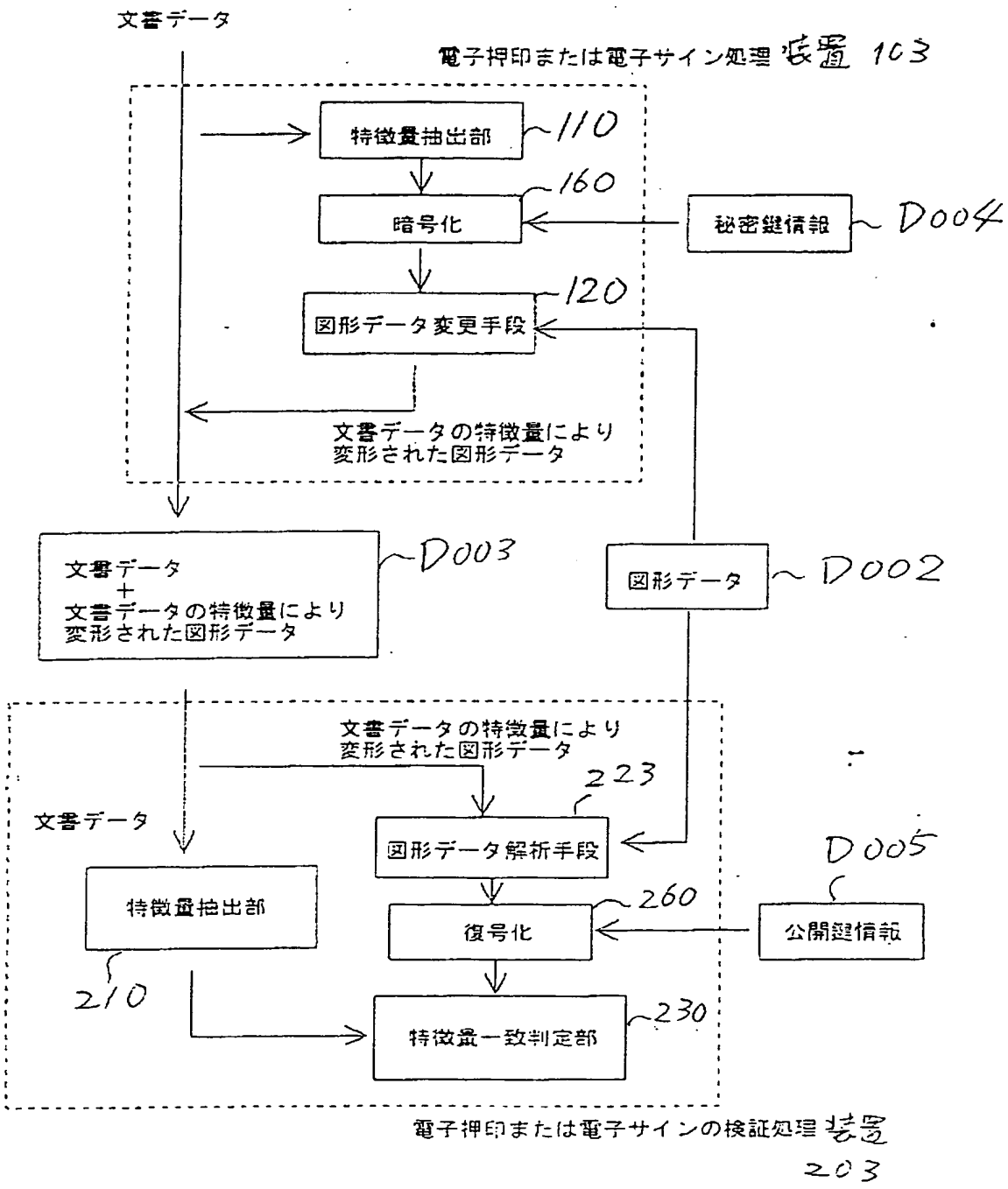
【図7】


文書データ D001
電子押印処理装置 102
131
押印位置
文書データ
141
印影データ 押印部
情報通信装置
152
位置検出部
印影データ
電子印鑑 301
321
位置指示部
310
D003
押印された電子文書
文書データ
特徴量抽出部
110
文書データ
＋
文書データの特徴量により
変形された印影データ
印影データ
121
印影データ
情報
通信部
印影データ
変更手段
D002
基準印影データ
（＋撹乱データ）
押印されている
印影データ
印影データ
一致判定部
231
一致判定結果
情報通信装置
252
202
電子押印の検証処理装置
文書データ
判定結果

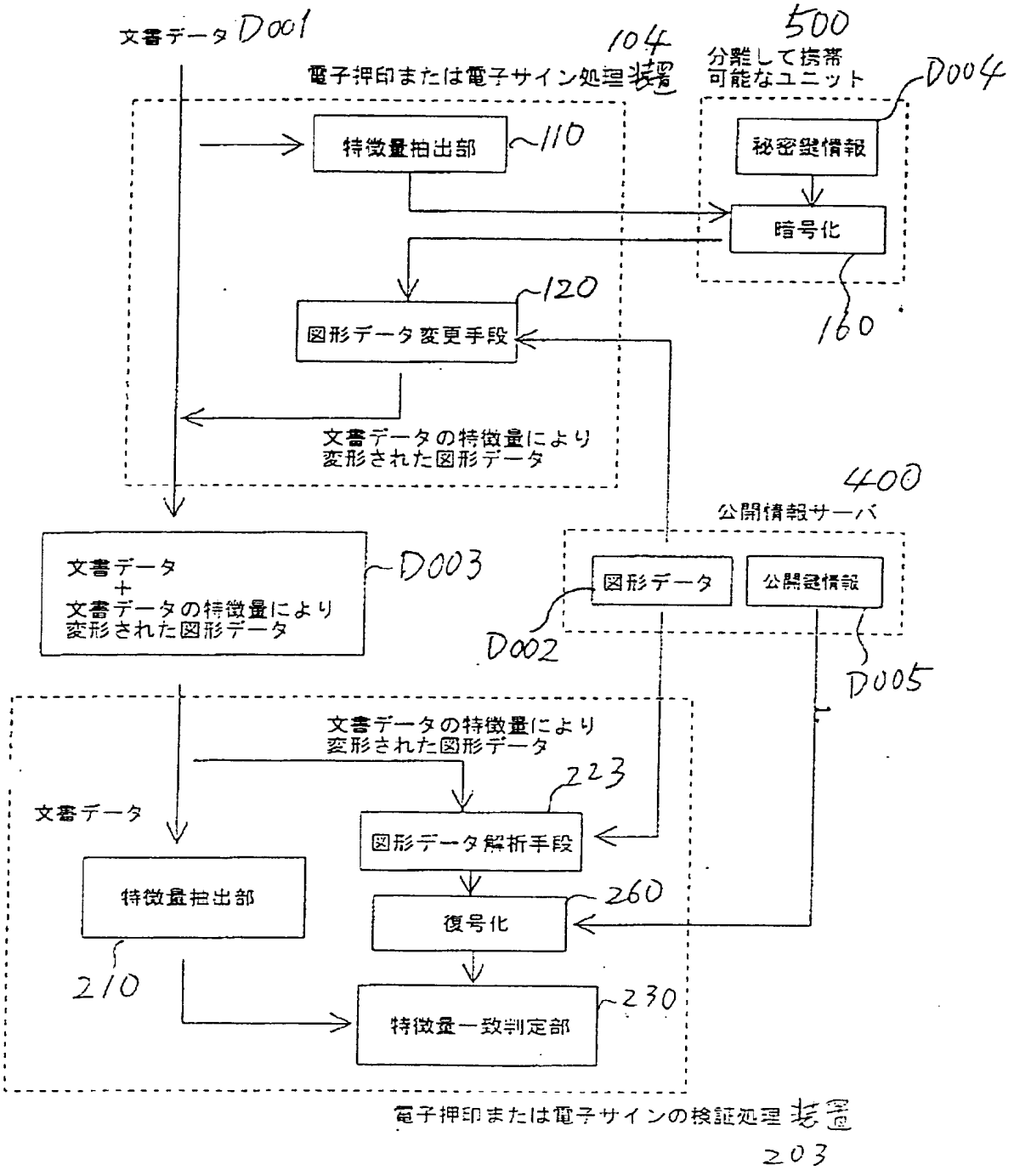
【図8】


文書データ D001
電子押印処理装置 102
131
印影データ 押印部
押印位置
印影データ
文書データ
152
情報通信装置
141
位置検出部
302
電子印鑑
322
情報 通信部
位置指示部 310
秘密鍵データ D004
D003
押印された電子文書
文書データ
暗号化処理部 111
文書データ + 文書データの特徴量により 変形された印影データ
暗号化された 文書データ
印影データ
印影データ 変更手段 122
基準印影データ
D002
印影データ
227
暗号化された 文書データの 抽出手段
基準印影データ
D002
232
文書データ
復号化された 文書データ
暗号化されている 文書データ
文書データ 一致判定部
復号化処理部
222
公開鍵データ
D005
電子押印の検証処理装置
203
公開情報格納装置
400
判定結果
文書データ

【図9】


文書データ
電子押印または電子サイン処理装置 103
特徴量抽出部
110
160
暗号化
秘密鍵情報
D004
120
図形データ変更手段
文書データの特徴量により
変形された図形データ
文書データ
＋
文書データの特徴量により
変形された図形データ
D003
図形データ
D002
文書データの特徴量により
変形された図形データ
223
文書データ
図形データ解析手段
D005
特徴量抽出部
260
復号化
公開鍵情報
210
特徴量一致判定部
230
電子押印または電子サインの検証処理装置
203

【図10】


文書データ D001
104
電子押印または電子サイン処理装置
500
分離して携帯可能なユニット
D004
特徴量抽出部
110
秘密鍵情報
暗号化
160
120
図形データ変更手段
文書データの特徴量により変形された図形データ
400
公開情報サーバ
文書データ
＋
文書データの特徴量により変形された図形データ
D003
図形データ
公開鍵情報
D002
D005
文書データの特徴量により変形された図形データ
223
文書データ
図形データ解析手段
特徴量抽出部
260
復号化
210
230
特徴量一致判定部
電子押印または電子サインの検証処理装置
203

【図１１】

従来例

(A)

```
This is the very important document.
No one can change this text.
```

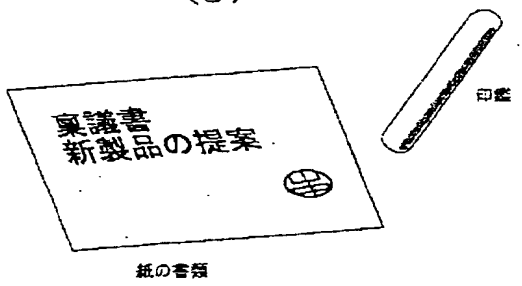
(B)

```
-----BEGIN PGP SIGNED MESSAGE-----

This is the very important document.
No one can change this text.
-----BEGIN PGP SIGNATURE-----
Version: 2.6.2i

iQCBAwUBMTwdb8HzgKtUlkkVAQHOVAL/XfzLATh98ast19h3qxBQErg13G5SgnE3
cxPDuqqN1YVQjStUiYQnSDZY4H+NXZVsgSjy2JewzpH+8eJrGt/YDtQFvBEw/Ja6
dUo/IY5r8FOBymx5uGd5cq82xrRMGFwN
=N6kh
-----END PGP SIGNATURE-----
```

(C)



フロントページの続き

(51)Int.Cl.⁶		識別記号	庁内整理番号	F I			技術表示箇所
G07F	7/12		7259−5J	G09C	1/00	640D	
G09C	1/00	640		G06F	15/62	455	
				G07F	7/08	B	
H04L	9/32			H04L	9/00	673D	
						675A	
				C07F	7/08	B	
						C	